vivendi

Whistleblower Guidelines

VIVENDI Group

November 2022

In accordance with the provisions of Articles 8 and 17 of French Law No. 2016-1691 of 9 December 2016 on transparency, combating corruption and the modernization of economic life (the "Sapin II Act"), as well as the provisions of French Law No. 2017-399 of 27 March 2017 on the duty of care of parent companies and contractors (the "Duty of Care Act"), Vivendi has established an alert system (the "System") which is a common platform for all the Group's entities: **alerte.vivendi.com.**

The System complies with the following:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons 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 specifically, French Law No. 2018-493 of June 20, 2018, on data protection and privacy, and the recommendations and decisions of the French Data Protection Authority (*Commission Nationale de l'Informatique et des Libertés* – CNIL).
- French National Agency for the Security of Information Systems (ANSSI) recommendations regarding information systems security; and
- French Anticorruption Agency (AFA) recommendations

The provisions of this procedure concerning the System, in particular the conditions relating to the protective status of whistleblowers, will be updated to conform to any regulatory changes that may occur after the implementation of the System.

1. The scope of the whistleblowing system

- **The system is available in both French and English and is available to any whistleblowers located in France and abroad.**

- This system is not intended to replace other existing internal (management, employee representative bodies, dedicated referents, human resources department, compliance officer) or external (e.g., the Human Rights Ombudsman) alert channels. Its use is an alternative to other alert channels, but is strongly recommended, given that the system guarantees the security and confidentiality of the processing of the alert.

- The whistleblower system is available to whistleblowers who wish to report any of the following information, breaches or infringements:

Report category	Information, breaches or infringements	Whistleblower category
	○ Conduct or situation in violation of Vivendi's anti-corruption code of conduct ○ Information relating to a crime or offence (including bribery) ○ Information about a threat or harm to general interest	○ Employees of Vivendi SE and its subsidiaries, as well as external and temporary employees ○ Individuals whose work contract has been terminated (provided that the information was obtained in the course of that contract)

Report made under Law No. 2016-1691 of December 9, 2016, known as the "Sapin II Act".	o Information concerning a violation or an attempt to conceal a violation of an international commitment duly ratified or approved by France, as well as a unilateral act of an international organization taken on the basis of this commitment o Information on a violation or an attempt to conceal a violation of European Union law, law or regulation (including violation of international sanctions or competition rules)	o Persons applying for employment with the relevant business unit (provided the information was obtained in connection with the application) o Shareholders, partners and holders of voting rights in the entity's shareholders' meeting o Members of the administrative, management or supervisory bodies o Co-contractors of the relevant business unit, their subcontractors or, in the case of legal persons, members of the administrative, management or supervisory bodies of such co-contractors and subcontractors, as well as their staff members
Report made under Law No. 2017-399 of March 27, 2017, known as the "Duty of Vigilance Act"	This concerns any of the following infringements relating to the activities of Vivendi SE or its subsidiaries, subcontractors or suppliers of the group: o Serious infringement of human rights and fundamental freedoms (including discrimination, moral and sexual harassment o Serious prejudice to the health and safety of individuals o Serious prejudice to the environment	o Any natural or legal person

Alerts pertaining to facts subject to national defense secrecy, medical secrecy, legal investigation or prosecution secrecy, and lawyer's professional secrecy are excluded from the scope of application.

2. Whistleblowing system arrangements

2.1 – The whistleblower

➢ Any originator of an alert benefits from the protective status of whistleblower upon meeting the following conditions:

- **To be a natural person**
- **Act in good faith:** The whistleblower must not be motivated by an intention to cause harm to others.
- **Act without financial compensation:** The whistleblower cannot claim to be paid for his or her alert.
- **Knowledge of facts:** Within a professional context, the whistleblower may report facts of which he/she has personal knowledge, or which have been reported to him/her. Outside the professional context, the whistleblower must have personal knowledge of the facts he/she is reporting.

- **Be recognizable:** The use of the system is subject to the identification of the whistleblower. As an exception, anonymity is allowed if the seriousness of the facts reported is established and if the facts are sufficiently detailed. The whistleblower will only be able to benefit from the protection measures (see below) once his/her anonymity has been lifted.

➢ Whistleblower protection

The whistleblower suffers no consequences for his or her alert

- Provided that they issue a warning in compliance with the provisions of this guide, whistleblowers may not be subject to any form of retaliation, nor to any threats or attempts to have recourse to such measures, in particular in the following forms (art. 10-1 of the Sapin II Act):

  - Suspension, layoff, contract termination or similar action
  - Demotion or promotion refusal
  - Transfer of duties, workplace relocation, wage reduction, change in working hours
  - Training suspension
  - Negative performance evaluation or work certificate
  - Disciplinary action initiated or enforced, admonishment or other sanction, including financial sanction
  - Coercion, intimidation, harassment, or ostracism
  - -Discriminatory, disadvantageous, or unfair treatment
  - Failure to convert a fixed-term or temporary contract of employment into a permanent contract, provided the employee had a legitimate expectation of being offered a permanent position
  - Failure to renew or early termination of a fixed-term or temporary employment contract
  - Prejudice, including attacks on the reputation of the person, in particular on an online public communication service, or financial penalties, including loss of activities and loss of income
  - Blacklisting on the basis of a formal or informal industry-wide or sectoral agreement, which may imply that the individual will not find future employment in the sector or industry
  - Early termination or cancellation of a contract for goods or services; " 14o Termination of a license or permit"
  - Abusive referral to psychiatric or medical treatment.

- Whistleblowers benefits from civil and criminal non-liability
  - Whistleblowers are not liable under civil law and may not be ordered to pay any compensation for damages caused by their reporting or public disclosure, provided they had reasonable grounds to believe that the reporting or public disclosure of the information was necessary to protect the interests at stake
  - Whistleblowers are not criminally liable if they infringe on a secret protected by law, provided that the disclosure is necessary and proportionate to protect the interests at stake, that it is made in compliance with the reporting procedures defined by law and that the person meets the criteria for whistleblowers set out in the law.

- This protective status also applies to natural or legal persons who are in contact with the whistleblower:
  - Facilitators: a natural or legal person of private, not-for-profit status who assists in the reporting or disclosure e.g.: union representatives, staff representatives
  - Natural person in contact with the whistleblower e.g.: colleagues, relatives
  - Legal bodies controlled by the whistleblower for which he/she works or is connected to in a professional context

The whistleblower's identity is not to be disclosed.

The system guarantees absolute confidentiality of the whistleblower's identity, of the persons whom the alert is addressed to and of any documents collected through the system. Unless the case must be disclosed to legal authorities:

- Any element that could allow the whistleblower to be identified shall not be disclosed without formal consent.
- Any element that could allow any person against whom the alert has been raised shall not be disclosed before the alert is deemed legitimate and proven.

2.2 – The implicated person

➢ Informing and protecting the implicated person

As soon as the data concerning him or her is recorded, the person implicated in the alert must be informed of the processing of this data to enable them to exercise their rights to access, oppose, rectify or delete the data. When protective measures must be taken to prevent the destruction of evidence, the person implicated in the alert will be informed after the fact.

The person who is the subject of the alert may not know the whistleblower's identity under any circumstances.
The identity of the person implicated in an alert will be treated in strict confidence. Any information that could identify the person implicated in an alert may not be disclosed, except to the judicial authorities, if after investigation it is established that the alert is well-founded.

2.3 - Protection of personal data

➢ The whistleblower's and the implicated person's rights of access, rectification and deletion (see Appendix 1)

In the context of the use of the System, every individual has the right to request access to their personal data, to have it rectified and, if the conditions are met, to have it deleted, to limit the processing of their data, the right to object to such processing and the right to portability of their data. Any person concerned may exercise their rights by writing to the e-mail address privacy@vivendi.com, precisely setting out their request and enclosing proof of identity. In any case, any concerned person may, at any time, refer to the competent authority (the CNIL) for any claim or complaint regarding the processing of their personal data.

➢ Anonymization and retention of personal data

Three cases are to be distinguished:

- The alert does not fall within the scope of the whistleblowing system → The alert and all related personal data must be anonymized within a maximum period of two (2) months following the closure of the admissibility process relating to such alert.
- The alert is deemed admissible, but no action is taken → The alert and all related personal data must be anonymized within a maximum of two (2) months following the closure of the verification process relating to such alert.
- The alert is deemed admissible, and action is taken on it, in particular the initiation of disciplinary action or litigation proceedings against the implicated person and/or the author of the alert → The alert and all related personal data must be kept until the end of the proceedings. They are then archived for the duration of the statute of limitations applicable to the facts reported.

Please note that the data is stored in the form of an intermediate archive and that the archived data can only be consulted on a one-off basis authorized personnel of Vivendi and/or the subsidiary concerned. The archiving periods are determined based on the category of facts reported.

3. Raising an alert

3.1 Submitting the alert

The whistleblowing system implemented by Vivendi Group allows alerts to be made based on the categories of facts defined on the whistleblowing platform. Each report can address only one event. To report several events, you must create one alert for each of them.

Abusive use (e.g., making false accusations) or use of the System with bad intent can result in disciplinary action as well as legal actions being taken against the perpetrator.

➢ **When submitting the alert on the platform, the whistleblower must:**

- Enter the information relating to his/her identity (unless he/she wishes to remain anonymous)
- Attach to the alert any document or information that could help substantiate the alleged facts (image, pdf, video of a maximum duration of X minutes)
- Provide all necessary and additional data requested

Enter his/her email address. A pop-up window appears upon registration of the alert specifying the file number assigned and the identifier as well as the link allowing the alert's originator to create a password allowing him/her to access his/her personal space.

A whistleblower may remain anonymous under two conditions:

- The seriousness of the facts mentioned is proven
  AND
- The factual elements detailed enough

Should the alert's originator prefer to remain anonymous, a pop-up window will appear upon registration of the alert specifying the file number assigned and the identifier, as well as the link enabling the alert's originator to create a password enabling him/her to access his/her personal space via the System. This pop-up window also includes a link to download the receipt confirming registration of the alert.

➢ **Informing the whistleblower**

As soon as the report is filed on the alert platform:

- The whistleblower receives an acknowledgement of receipt notifying him/her of the registration of his/her alert within a maximum of 7 days,
- The whistleblower is notified within a maximum of 3 months of the receipt acknowledgement of the measures being considered or taken to assess the accuracy of the allegations and, if necessary, to address the matter reported. By connect to his/her personal space, he/she may follow the progress of the processing of the alert at any time:
  - If the alert is not receivable → The file is closed for inadmissibility.
  - If the alert is admissible → The main referent transfers the alert to the competent Investigation Commisssion with regard to the nature of the facts reported, which conducts the necessary investigations and, if necessary, implements the appropriate measures.
- The processing time is extended to six months if specific circumstances of the alert, linked in particular to its nature or complexity, require additional investigations. The whistleblower is notified before the expiry of the initial three-month period

➢ **Procedures for exchanging information with the whistleblower**

Whistleblowers have an online discussion space where they can exchange information with a person in charge of their alert and send additional documents and evidence. The Group takes great care to ensure that the evidence or documents collected are filed on the whistleblowing platform in order to guarantee the confidentiality and security of these documents.

3.3 - Receipt and review of the alert

Upon registration of the report on the alert platform, the Principal Alert Referent (PAR) is made aware of the alert through the platform available to employees (alert.vivendi.com) and informs Vivendi's Compliance Department which notifies the local Compliance Officer of the receipt of an alert concerning their subsidiary. The latter supports the PAR in assessing the admissibility of the alert.

The PAR reviews the admissibility of the alert from the date of its receipt on the platform:

- Characteristics of the alert
- Information provided in the report
- Criteria applicable to the whistleblower (cf.§2.1).

At each stage of the alert processing, the whistleblower receives a notification to connect to his case and find out the current status:

Status	File status details
Pending	The alert has been successfully registered on the platform and must be reviewed to determine its admissibility
Processing	The alert has been qualified as admissible by the referent and is being processed by the Investigation Commisssion
Closed -Arhcived	The alert file has been closed and archived
Closed - Anonymized	The alert case has been closed and all personal data has been anonymized

➢ The request for additional documents via the platform

If the alert submitted by the whistleblower on the platform is not sufficient to determine its admissibility, the PAR may ask the whistleblower for supporting or additional documents (through an online discussion area). In this way, he/she may be asked to provide a document justifying his/her status as a whistleblower (employee, shareholder, etc.) and any other element that may help to assess the accuracy of the allegations.

3.4 – The conduct of the internal investigation

➢ Information and decision to conduct an investigation by the Investigation Commission

Once an alert is deemed admissible, the PAR transfers it to the "anti-corruption/vigilance" Investigation Commission or the "anti-harassment" Investigation Commission. The relevant Investigation Commission gathers its members (the secondary referents), made up of representatives of the head office and representatives of the subsidiaries concerned, who have the necessary expertise to address the alert.

When there are conclusive facts

Based on the analysis of the information gathered by the PARs, the Committee of Inquiry may find that there is sufficient evidence or facts to warrant an investigation.

When there is lack of evidence

If based on the analysis of the information gathered by the PAR, the Investigation Unit cannot confirm the facts reported by the whistleblower, it will either decide to:

- Request additional information and documents, or

- Close the alert.

➢ Conducting an investigation

Based on the information gathered, the Committee of Inquiry decides to open an investigation in conjunction with the Compliance Officer of the subsidiary concerned, who will involve representatives of the subsidiary that he deems necessary to assist in the investigation (HR department, legal department, financial department, etc.). An independent expert may be called in to carry out all or part of the investigation, particularly where complex elements are involved (e.g., IT expertise, accounting audit, etc.).

The investigation is carried out with respect for the confidentiality of the author of the alert, the implicated person(s) and the information gathered. It is carried out in compliance with the requirements linked to existing investigation procedures, in particular investigations concerning social matters.

➢ **Conducting interviews**

Interviews are conducted by the Compliance Officer, or any other person designated for this purpose. They guarantee absolute confidentiality and aim to verify the facts surrounding the alleged involvement of the implicated person. Any person likely to provide information that may help determine whether the allegations against the implicated person are true may be interviewed as part of the investigation.

The implicated person is entitled to defend themselves in order to determine the accuracy of the facts.

At the end of the hearing, a report will be drawn up by the Compliance Officer or any other person designated for this purpose, which is validated by the implicated person and attached to the investigation report. The implicated person is kept informed of the outcome of the investigation.

➢ **Drawing up of an investigation report and decision of the Investigation Unit**

A report must be drawn up at the end of the investigations carried out in the context of the alert. This report is given to the Committee of Inquiry, which decides on the follow-up actions to be taken.

3.5 - Follow-up to the investigation

- The investigation report does not confirm the facts reported by the whistleblower, the Investigation Commission closes the alert. The whistleblower is informed of the classification of the alert and the motives behind it by a message posted on the whistleblowing platform.

- If the investigation report only partially confirms the facts reported, the Investigation Commission may request additional investigations within a further 3-month period. The whistleblower is informed by a message posted on the whistleblowing platform of the continuation of the investigations at the end of the 3-month initial period.

- At the end of the investigations, the investigation report demonstrates that there is sufficient evidence to confirm the facts that have been reported. The whistleblower is informed, by means of a message posted on the whistleblowing platform, of the measures considered or taken to assess the accuracy of his or her allegations and, if applicable, of the measures to address the reported facts, as well as the motives for these measures.

All the elements relating to the processing of the alert (investigation report, opinion of the Commission of Inquiry, follow-up given to the alert) are saved and classified according to the internal rules for the protection of personal data.

Two e-mail addresses are associated with the alert system platform:

compliance@vivendi.com : the sole purpose of this e-mail account is to allow the whistleblower to discuss the functioning of the platform (e.g., loss of login and/or password)

privacy@vivendi.com : the sole purpose of this e-mail account is to allow the whistleblower to request access to, or rectification or deletion of his/her personal data.

The recipients of e-mails sent to this address are in charge of the administration of the site (*webmaster*). They do not have access to the alerts registered on the platform or to information related to the processing of such alerts.

Appendix 1 – Protection of personal data

Whistleblowing system

In accordance with Law No. 2016-1691 of 9 December 2016 on transparency, combating corruption and the modernization of economic life (the "Sapin II Act") and Law No. 2017-399 of 27 March 2017 on the duty of care of parent companies and contractors (the "Duty of Care Act"), the Vivendi Group (the "Group") implemented a whistleblowing system.

In accordance with Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data (the "GDPR") and Law No. 78-17 of 6 January 1978 on Information Technology, Data Files and Individual Liberties as amended (the "French Data Protection Act"), detailed information concerning any processing carried out under this system is provided below.

The terms used below, whether in the singular or plural, beginning with a capital letter shall, unless otherwise expressly defined in this procedure document, have the meaning given to them by Article 4 of the GDPR.

I. Identity of the data controller

When the alert is raised by an employee or external collaborator of Vivendi SE and/or relates to facts that only concern its employees or collaborators, Vivendi SE (42, Avenue de Friedland - 75380 Paris Cedex 08 - Tel: 01 71 71 10 00) acts as the Data Controller.

When the alert is made by an employee or external collaborator of any of Vivendi SE's subsidiaries and/or concerns matters relating to its employees or collaborators, Vivendi SE and the subsidiary concerned act as joint data controllers. For contact information regarding the subsidiary, please refer to the relevant subsidiary's corporate website.

II. Purposes and legal bases of the processing

The purpose of the whistleblowing system is to receive alerts relating to conduct or situations that contravene the applicable laws and regulations, in particular, corruption or influence peddling, anti-competitive practices, violation of economic sanctions, infringement of human rights and fundamental freedoms, endangering the health or safety of others, damage to the environment and discrimination or psychological or sexual harassment and to handle such reports in an appropriate manner.

Vivendi SE has implemented this system to comply with the provisions of the Sapin II Act and the Duty of Vigilance Act. It also serves the legitimate purpose of keeping it and its subsidiaries informed and able to act promptly and appropriately in the event of a violation of any applicable laws and regulations.

III. Recipients

Personal data collected via the whistleblowing system are sent to the main contact person in charge of investigating the admissibility of the alert and to their deputy.

If the alert is deemed admissible, the Personal Data is then transmitted to the Secondary Referents, specially designated and authorized to process and manage the alert according to the nature and qualification of the facts it contains, as well as to a limited number of Vivendi SE employees, and where applicable, to the subsidiary concerned, specifically identified and designated for the purpose of managing and processing the alert.

Any Personal Data collected and processed in the context of the whistleblowing system may, where applicable, be consulted by a limited number of authorized persons within the Information Services Department of Vivendi SE, the Legal, CSR and Compliance Departments as well as the General Management of Vivendi SE and/or any of the subsidiaries concerned by the alert.

In addition, it is possible that in the course of handling an alert, access to personal data may be given to third-party providers, who are subject to a contractual confidentiality commitment.

IV. Personal data retention period

Personal Data collected and processed within the framework of the whistleblowing system are kept only for the time strictly necessary for the purposes for which they were collected.

- When the alert is deemed inadmissible, the related Personal Data are anonymized within a maximum of two (2) months following the closure of the admissibility process relating to such alert.
- When the alert rt is deemed admissible, but no action is taken, the Personal Data relating to it shall be anonymized within two (2) months following the end of the verification process relating to such alert.
- When the alert is deemed admissible and action is taken on it, in particular when disciplinary action or litigation proceedings are initiated against the person implicated in the alert and/or the author of the alert, the related Personal Data are kept until the end of the proceedings. At the end of this procedure, the Personal Data is archived for the duration of the legal statute of limitations applicable to the facts reported or any other mandatory retention period resulting from a legislative or regulatory text. At the end of this archiving period, the Personal Data is then anonymized.

Details on the applicable archive retention periods can be found in Appendix 2.

V. Rights of concerned persons

Pursuant to Articles 15 et seq. of the GDPR, any Data Subject whose Personal Data is collected and processed via the whistleblowing system has the right to request from Vivendi SE or any of its subsidiaries when the alert is made by one of its employees or one of its external collaborators or when the facts reported concern such subsidiary access to their Personal Data, its rectification and, if the conditions are met, its deletion, a limitation of its processing, the right to object to said processing and the right to the portability of their Personal Data. Moreover, in accordance with the French Data Protection Act, an implicated person has the right to define directives for the conservation, deletion and communication of their Personal Data after their death.

An implicated person may exercise their rights by writing to the following e-mail address: privacy@vivendi.com, precisely setting out their request and enclosing proof of identity.

In any case, implicated persons may refer to the French National Commission on Informatics and Liberty (CNIL) for any claim or complaint concerning the Processing of their Personal Data.

Appendix 2 – Archive retention periods

Categories of reported facts	Archive retention periods
Corruption	6 years
Influence peddling	6 years
Crime	30 years
Offence	6 years (10 years in case of personal injury)
Serious and manifest violation of an international commitment regularly ratified or approved by France, of a unilateral act of an international organization taken on the basis of such a commitment, of the law or of the regulations	To be determined case by case according to the applicable legal prescription period based on the violation committed
Threat or serious prejudice to the public interest	To be determined according to statutory limitation period applicable to the threat or damage concerned
Anti-competitive practices	5 years
Violation of economic sanctions	To be determined according to the applicable statutory limitation period based on the violation committed
Violation of human rights and fundamental freedoms	6 years (10 years in case of personal injury)
Endangerment of the health or safety of others	6 years (10 years in case of personal injury)
Damage to the environment	10 years
Discrimination, moral or sexual harassment	6 years (10 years in case of personal injury)
Violation of the Group's Anticorruption	To be determined according to the applicable statutory limitation period based on the violation committed