Procedure exposing the receipt and processing of alerts for whistleblowers

VIVENDI Group

February 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 implemented within the Vivendi Group covers alerts related to the following breaches and violations:

- **Breaches of the Anti-Corruption Code (Article 17 of the Sapin II Act)**
  - Conduct or situations that may constitute corruption or influence peddling in breach of the Group's Anti-corruption Code.

- **Other wrongdoings (Article 6-1 of the Sapin II Act)**

  - A crime or offence;
  - A serious, blatant violation of an international commitment duly ratified or approved by France ;
  - A serious, blatant violation of a unilateral action taken by an international organization on the basis of a duly ratified international treaty or convention;
  - A serious, blatant violation of the law or a regulation; and
  - A serious threat or prejudice to the general interest, of which the whistleblower has first-hand knowledge.

Facts, information or events covered by national defence secrecy, doctor/patient confidentiality or lawyer/client privilege are specifically excluded from the whistleblowing procedure (Article 6-2 of the Sapin II Act).

- **Serious violations of human rights and fundamental freedoms** (including discrimination, moral and sexual harassment), **the health and safety of individuals and the environment resulting from the activities of the Group or those of its subcontractors and suppliers with whom they have an established business relationship (Article 1 of the Duty of Care Act).**

- **Other violations**: anti-competitive practices, violation of international economic sanctions.

2. Whistleblowing arrangements

2.1 – The whistleblower

The following are considered whistleblowers:

- Employees of Vivendi and its subsidiaries as well as their external and occasional collaborators in order to report any conduct or situations contrary to the group's Anti-Corruption Code, in accordance with Article 17 of the Sapin II Act;

- Employees of Vivendi and its subsidiaries as well as their external and occasional collaborators, in order to report a crime or offence, a serious and manifest violation of an international commitment duly 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 a regulation, or a serious threat or prejudice to the general interest, in accordance with Article 6 of the Sapin II Act;

- Employees of Vivendi and its subsidiaries as well as their external and occasional collaborators in order to report the existence of anti-competitive practices or violations of international economic sanctions in connection with the Group's activities; and

- Any person, in order to report a serious violation of human rights and fundamental freedoms (including discrimination, moral and sexual harassment), the health and safety of individuals and the environment resulting from the activities of Vivendi or its subsidiaries, as well as from the activities of their subcontractors or suppliers with whom they have an established business relationship, in accordance with the Duty of Care Act.

➢ Conditions applicable to the whistleblower to benefit from protected status in the context of filing an alert

In the context of alerts raised in connection with Sapin II Act, the whistleblower is granted protected status subject to four cumulative conditions:

- The whistleblower must be a **natural person**;
- The whistleblower must **have a first-hand knowledge** of the events or facts disclosed or reported *(he or she cannot, therefore, act as an intermediary but can only report suspicious facts or events he or she has personally witnessed);*
- The whistleblower must **act selflessly** *(i.e., the individual receives no benefit or financial reward in return for raising an alert).*
- The whistleblower must act in **good faith** *(facts or events must not be disclosed or reported with malicious intent).*

➢ Whistleblower protection

A whistleblower will not suffer any consequences related to their alert

A whistleblower who is a natural person, acting in good faith and selflessly, may not be dismissed, sanctioned or discriminated against in any way for having reported facts in accordance with this procedure, even if the facts subsequently prove to be unfounded or no further action is taken.

Conversely, abuse of the system can lead to disciplinary measures and, potentially, legal action.

A whistleblower's identity will not be disclosed

The System guarantees strict confidentiality of the identity of the whistleblower, of the persons implicated in the alert and of all the information and documents collected via the System. Except in the case of communication to the judicial authorities:

- Information that might permit the identification of the whistleblower can only be disclosed with their consent.
- Information that might permit the identification of the person(s) implicated can only be disclosed once the validity of the alert has been established.

➢ A whistleblower is kept informed

The whistleblower is promptly informed of the receipt of the alert by an electronic message with acknowledgement of receipt. The Principal Alert Referent (PAR) then has:

- a reasonable period of time to decide on the admissibility of the alert; and
- A maximum of three months [3 months] to decide on the handling of the alert and to inform the whistleblower by e-mail of the action planned or taken in response to the alert. This timeframe is not intended to be a deadline for the complete closure of the alert.

If an alert is deemed inadmissible or is not pursued, the whistleblower, and the implicated person, if he or she has been informed of an alert concerning him or her, are informed of the closure of the admissibility process and/or the verification of the facts reported. They are also informed that the data will be destroyed or archived, after anonymization, within two months [2 months] of the closure of the admissibility or verification process. [the French is different here so I updated the English to match the French].

➢ Communication with a whistleblower

The group provides whistleblowers with an online discussion area where they can speak with the person in charge of their whistleblowing case and send additional documents and evidence. The group remains very vigilant as to the gathering of evidence or documents which must be deposited on the whistleblowing platform to guarantee the confidentiality and security of these documents.

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.

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

- Enter the information relating to their identity (unless they wish to remain anonymous)
- Attach to the alert any document or information that could help substantiate the alleged facts
- Provide all necessary and additional data requested

When the author of the alert has entered their e-mail address:

- A pop-up window appears when the alert is registered giving the file number assigned and the identifier as well as the link allowing the author of the alert to create a password enabling them to access their personal area via the System; and
- An automatic confirmation message will be sent to the alert's author as soon as their alert is registered, which includes the assigned file number and the identifier as well as the same link allowing the author of the alert to create their password

enabling them to access their personal area via the System. This message also includes the confirmation of receipt of the alert.

A whistleblower may remain anonymous under two conditions:

- The seriousness of the facts mentioned is established;
  AND
- The factual information is sufficiently detailed.

When the author of the alert wishes to remain anonymous, a pop-up window appears when the alert is registered. It specifies the file number assigned and the identifier, as well as the link enabling the author of the alert to create a password enabling them to access their personal space via the System. This pop-up window also includes a link for downloading the confirmation of receipt of the alert.

➢ **Once the alert is registered in the platform**

The whistleblower can connect to their case file to follow the processing of their alert by tracking changes in its status:

Status	**Definition**
Pending	The alert has been registered on the platform and will be reviewed to determine its admissibility
In progress	The alert has been qualified as admissible by the PAR and is being processed by the Investigation Unit.
Closed - Archived	The alert case file has been closed and archived
Closed - Anonymized	The alert case file has been closed and all personal data has been anonymized

3.2 – Whistleblower's exemption from liability

[When acting in good faith] A whistleblower is exempt from criminal liability for disclosing secret information when such disclosure (i) is necessary and proportionate to the protection of the interests in question; (ii); respects the whistleblowing procedure; and (iii) is made by a person who meets the criteria for classification as a whistleblower.

The disclosure of a national defense secret, a medical secret or a secret arising from relations between a lawyer and their client is excluded from this exemption from criminal liability.

3.3 - Receipt and review of the alert by the Principal Alert Referent (PAR)

The Principal Alert Referent (RPA) 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 whistleblower receives an acknowledgement of receipt after registering their alert**

The PAR starts to review the admissibility of the alert from the date of reception on the platform.

The whistleblower can track the progress of their alert on the platform via the following indications:

- Pending
- In progress
- Closed - Archived
- Closed - 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).

If the alert case is closed, the investigative information have to be anonymised within 2 months. If the investigation continues, this information is transmitted to the Investigation Unit.

3.4 – The conduct of the internal investigation

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

Once an alert is deemed admissible, the PAR transfers it to the Compliance Investigation Unit or the HR Investigation Unit, as appropriate. The relevant Investigation Unit holds a meeting of its members (the secondary referents) made up of representatives from the head office and the subsidiaries concerned.

When there are conclusive facts

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

When there is insufficient 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 Investigation Unit decides to open an investigation in conjunction with the Compliance Officer of the subsidiary concerned, who will involve representatives of the subsidiary to assist in the investigation. 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 Investigation Unit, which decides on the follow-up actions to be taken.

If there is insufficient evidence: The Investigation Unit cannot confirm the facts reported by the whistleblower and decides to close the alert.

If there is conclusive evidence: The Investigation Unit may find that there is sufficient evidence to support the facts reported by the whistleblower. In this case, it issues an opinion on the action to be taken, which is transmitted to the Chief Compliance Officer.

3.5 - Follow-up to the investigation

All the elements relating to the handling of the alert (investigation report, opinion of the Investigation Unit, suggestions for follow-up) are sent to the Group Chief Compliance Officer, who validates the decision to take disciplinary action or initiate legal proceedings.

The Chief Compliance Officer informs the Chairman of Vivendi's Management Board of the action taken in response to the alert.

E-mail addresses are associated with the alert system platform:

alerte@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)

Priavcy@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 Care 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.

For further details on the applicable archive retention periods, please refer to Appendix 2.

V. Rights of data subjects

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