HAVAS

WHISTLEBLOWER GUIDELINES

Contents

Introduction

In accordance with the provisions of articles 8 and 17 of French law No. 2016-1691 of December 9, 2016 on transparency, the fight against corruption and the modernisation of economic life known as the "Sapin II law", as well as the provisions of French law No. 2017-399 of March 27, 2017 on the duty of care of parent companies and contractors known as the "Duty of care law", Havas has established an alert system (the "System") which is a common platform for all the Group's entities available on the intranet and on the following website at the following address: havas.integrityline.com

Employees may also submit an alert directly to the Compliance Department at the following address: compliance@havas.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. 78-17 of January 6, 1978 as amended, on Data Processing, Data Files and Individual Liberties as well as the guidelines on whistleblowing systems and and the recommendations and decisions of the French Data Protection Authority (Commission Nationale de l'Informatique et des Libertés – CNIL); and

- French Anticorruption Agency (AFA) recommendations.

The provisions of this procedure concerning the System, will be updated to comply with any regulatory changes that may occur after the implementation of the System.

1

1. THE SCOPE OF THE WHISTLEBLOWING SYSTEM

1. THE SCOPE OF THE WHISTLEBLOWING SYSTEM

The System is available in french, english and spanish. It is available to 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, Chief 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 System is available to whistleblowers who wish to report any of the following information, breaches or infringements:

REPORT CATEGORY	INFORMATIONS, BREACHES OR INFRINGEMENTS	WHISTLEBLOWER CATEGORY
REPORT MADE UNDER LAW NO. 2016-1691 OF DECEMBER 9, 2016, KNOWN AS THE "SAPIN II LAW"	• Conduct or situation in violation with Havas anti-corruption Code • Information relating to a crime or an offence (including acts of corruption) • Information about a threat or harm to general interest • 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 • 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)	• Employees of Havas and its subsidiaries, as well as external and occasional employees • Individuals whose work contract has been terminated (provided that the information was obtained in the course of that contract) • Persons applying for employment within the relevant business unit (provided that the information was obtained in connection with this application) • Shareholders, partners and holders of voting rights in the entity's shareholders' meeting • Members of the administrative, management or supervisory bodies • 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 LAW"	This concerns any of the following infringements relating to the activities of Havas or its subsidiaries, subcontractors or suppliers of the group: • Serious infringement of human rights and fundamental freedoms (including	• Any natural or legal person

REPORT CATEGORY	INFORMATIONS, BREACHES OR INFRINGEMENTS	WHISTLEBLOWER CATEGORY
REPORT MADE UNDER LAW NO. 2017-399 OF MARCH 27, 2017, KNOWN AS THE "DUTY OF VIGILANCE LAW"	discrimination, moral and sexual harassment) • Serious prejudice to the health and safety of individuals • Serious prejudice to the environment	

Alerts pertaining to facts, information or events covered by national defence secrecy, medical secrecy, legal investigation or prosecution secrecy, and lawyer's professional secrecy are excluded from the scope of application (Article 6-2 of the Sapin II law).

2

2. WHISTLEBLOWING SYSTEM TERMS & CONDITIONS

2. WHISTLEBLOWING SYSTEM TERMS & CONDITIONS

A. The whistleblower

The author of the alert benefits from the protective status of whistleblower if the following conditions are met:

- **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 or she has personal knowledge or which have been reported to him or her. Outside the professional context, the whistleblower must have personal knowledge of the facts he or 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 or her anonymity has been lifted.

WHISTLEBLOWER'S PROTECTION

The whistleblower suffers no consequences for his or her alert

- Provided that they issue an alert in compliance with the provisions of these guidelines, 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 (Article 10-1 of the Sapin II law):
  - — 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;
  - — Termination of a license or permit;
  - — Abusive referral to psychiatric or medical treatment.

• Whistleblowers benefit 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 to be considered as a whistleblower set out in the law.

• This protective status also applies to natural or legal persons who are in contact with the whistleblower:
  — Facilitators: non profit making natural or legal person 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 or she works or is connected to in a professional context.

• The System guarantees absolute confidentiality of the whistleblower's identity, of the persons concerned by the alert and of any information or 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 lead to the identification of the person(s) concerned by the alert shall not be disclosed before the alert is deemed legitimate and proven.

B. The person concerned by the alert

INFORMING AND PROTECTING THE PERSON CONCERNED BY THE ALERT

As soon as the data concerning him or her is recorded, the person concerned by the alert must be informed of the processing of this data to enable him or her to exercise his or her rights to access, rectify and if conditions are met, oppose, delete the data, limit their processing or exercise their portability right. When protective measures must be taken to prevent the destruction of evidence, the person concerned by the alert will be informed after the fact.

The person concerned by the alert cannot know the whistleblower's identity under any circumstances at this stage.

The identity of the person concerned by the alert will be treated in the strictest confidence. Any information enabling the identification of the person concerned by the alert may not be disclosed, except to the judicial authority, if after investigation it is established that the alert is well-founded.

C. Protection of personal data

RIGHTS OF ACCESS, RECTIFICATION AND DELETION (SEE APPENDIX 1)

When using the System, every individual has the right to request access to his or her 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 his or her rights by writing to the e-mail address dpo@havas.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 for the protection of personal data (in France, the CNIL) for any claim or complaint regarding the processing of his or her personal data.

For more information on the individuals' rights, please refer to Appendix 1 of the present document: Information notice – Protection of personal data.

RETENTION AND ANONYMIZATION OF PERSONAL DATA

Three cases are to be distinguished:

• When the alert is deemed inadmissible, the 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.

• When the alert is deemed admissible but no action is taken, the related personal data must be anonymized within a maximum period of two (2) months following the closure of the verification process relating to such alert.

• When the alert is deemed admissible and action is taken on it, in particular the initiation of disciplinary action or litigation proceedings against the author of the alert and/or the person concerned by the alert, the 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 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.

Please note that the archived data can only be consulted on a oneoff basis authorized personnel of Havas and/or the subsidiary concerned. The archiving periods are determined based on the category of facts reported (see Appendix 2).

3

3. RAISING AN ALERT VIA THE SYSTEM

3. RAISING AN ALERT VIA THE SYSTEM

A. Submitting the alert

The System implemented by Havas Group allows alerts to be made based on the categories of facts defined on the whistleblowing platform. When filing an alert on the platform, it is possible to select several categories if the nature of the facts reported requires it.

Abusive use (e.g., making false accusations) or use of the System with bad intent can result in disciplinary actions 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 or her identity (unless he or she wishes to remain anonymous);
- Attach to the alert any document or information that could help substantiate the alleged facts (the authorized formats are: PDF, Word, Excel, Power Point, GIF, JPEG);
- Provide all necessary and additional data requested;
- Enter his or her e-mail address to confirm registration and create his or her personal password. A unique case ID reference will be assigned to him or her at the end of registration. Please ensure to keep your login and case ID reference to access the secure inbox. If you lose your case ID reference, you will not be able to reset your login details. You will have to submit a new alert.

A whistleblower may remain anonymous provided that:

- **The seriousness of the facts mentioned is proven**

AND

- **The factual elements are sufficiently detailed**

If the author of the alert wishes to remain anonymous, he or she will still need to create a personal password and ensure that he or she keeps the unique case ID reference assigned to him or her at the end of the alert registration process, in order to access the secure inbox.

INFORMING THE WHISTLEBLOWER

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

- Within a maximum of seven (7) days, the whistleblower receives an acknowledgement of receipt notifying him or her of the registration of his or her alert.
- The whistleblower is notified within a maximum of three (3) months from the acknowledgement of receipt of the measures planned or taken to assess the accuracy of the allegations and, if necessary, to address the matter reported. The whistleblower can follow the progress of the processing of the alert at any time through his or her personal space:
  - If the alert is inadmissible → The file is closed for inadmissibility.
  - If the alert is admissible → With regard to the nature of the facts reported and in compliance with the local procedures, the Group Compliance Department identifies and conducts the necessary investigations and, if necessary, implements the appropriate measures.
- The processing time is extended to six (6) months if specific circumstances of the alert, especially linked to its nature or complexity, require additional investigations. The whistleblower is notified before the expiry of the initial three-month (3) period.

PROCEDURES FOR EXCHANGING INFORMATION WITH THE WHISTLEBLOWER

The whislteblower has an online discussion space where he or she can exchange information with a Compliance referent in charge of his or her alert and send additional documents and evidence. The Group is very careful 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.

B. Receipt and review of the alert

Once the alert is registered on the alert platform (havas.integrityline.com), the Group Compliance Department is made aware and assesses the admissibility of the alert with regard to the following elements:

- Characteristics of the alert;
- Information provided in the report;
- Criteria applicable to the whistleblower (see §2.A).

The steps of the handling of the alert are as follows:

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 and is being processed by the Group Compliance Department
CLOSED – ARCHIVED	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 Compliance referent may ask the whistleblower to provide additional documents (through an online discussion area). Therefore, he or she may be asked to provide a document justifying his or her status as a whistleblower (employee, shareholder, etc.) and any other element that may help to assess the accuracy of the allegations.

C. The conduct of the internal investigation

INFORMATION AND DECISION TO CONDUCT AN INVESTIGATION BY THE COMPLIANCE DEPARTMENT

When an alert is deemed admissible, the Group Compliance Department prepares the investigation. There are two possible scenarios:

When there are conclusive facts
Based on the analysis of the information transmitted, the Group Compliance Department may find that there is sufficient evidence or facts to warrant an investigation.

When there is lack of evidence
Based on the analysis of the information transmitted, the Group Compliance Department 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 Group Compliance Department decides to open an investigation entrusted to a specially composed invetsigation unit based on the facts reported. To conduct this investigation, the Group Compliance Department may involve the following Departments depending on the required expertise: HR Department, Legal Department, Financial Department, Internal Audit Department, etc.
An independent expert, bound by confidentiality, may be called in to carry out all or part of the investigation, especially when there are complex elements (e.g., IT expertise, accounting audit, etc.).

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

CONDUCTING INTERVIEWS

Interviews are conducted by the investigation team, or any other person designated for this purpose guaranteeing absolute confidentiality. The aim of this interview is to verify the facts surrounding the alleged involvement of the person concerned by the alert. Any person likely to provide information that may help determine whether the allegations against the person concerned by the alert are true may be interviewed as part of the investigation.

In application of the adversarial principle, the person concerned by the alert has the right to be interviewed by the investigation team and to answer to all the grievances against him or her.

After each interview, a report will be drawn up by the investigation team or any person designated for this purpose. It will be validated and signed by each person interviewed and attached to the investigation report. If requested, the person concerned by the alert and its author are kept informed of the progress of the investigation.

DRAWING UP OF AN INVESTIGATION REPORT AND FOLLOW-UP

A report must be drawn up by the investigation team at the end of the investigations carried out as part of the alert. The investigation team shares the conclusions of the investigation report with the author of the alert and the person concerned by the alert.

D. Follow-up to the investigation

At the end of the investigations carried out by the investigation team and the drawing up of the investigation report, three situations may arise:

- **The investigation report does not confirm the facts reported by the whistleblower**

The investigation team closes the alert. The whistleblower is informed of its closure and the motives behind it by a message available on the whistleblowing platform.

- **The investigation report only partially confirms the facts reported**

The investigation team may benefit from an additional 3-month period to carry out further investigations. The whistleblower is informed by a message sent on the whistleblowing platform of the continuation of the investigations at the end of the 3-month initial period.

- **The investigation report demonstrates that there is sufficient evidence to confirm the facts reported**

The whistleblower is informed, by 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 investigation team, 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 complementary with the alert system platform:

compliance@havas.com: the sole purpose of this e-mail account is to allow the whistleblower to discuss the functioning of the platform, if the alert was made via the System.

dpo@havas.com: the sole purpose of this e-mail account is to allow the whistleblower to request access to, or exercise the right of rectification, limitation of processing, protability or deletion of his or her personal data, if conditions are met.

Requests made to the above two addresses do not grant access to the platform's content.

These email addresses are an external relay between requests made via them and their management by the Data Controller of the alert platform.

4

4. APPENDIX 1 - INFORMATION NOTICE - PROTECTION OF PERSONAL DATA

4. APPENDIX 1 - INFORMATION NOTICE - PROTECTION OF PERSONAL DATA

In accordance with law No. 2016-1691 of December 9, 2016 on transparency, the fight against corruption and the modernisation of economic life (the "Sapin II law") and law No. 2017-399 of March 27, 2017 on the duty of care of parent companies and contractors (the "Duty of care law"), the Havas Group (the "Group") has implemented a whistleblowing system (the "System").

In accordance with Regulation 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 and the free movement of such data (the "GDPR") and law No. 78-17 of January 6, 1978 on Data Processing, 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.

A. Identity of the Data Controller

When the alert is raised by an employee or external collaborator of Havas and/or relates to facts that only concern its employees or collaborators, Havas (29-30 Quai de Dion Bouton – 92800 Puteaux - France) acts as the Data Controller.

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

B. Purposes and legal bases of the processing

The purpose of the 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.

Havas has implemented this System to comply with the provisions of the Sapin II law and the Duty of care law. 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.

C. Recipients

Personal data collected via the System are sent to the Principal Alert Referrent 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 Havas 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 System may, where applicable, be consulted by a limited number of authorized persons within the Information Services Department of Havas, the Legal, CSR and Compliance Departments as well as the General Management of Havas 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.

D. Personal data retention period

Personal data collected and processed within the framework of the 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 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 concerned by the alert and/or the author of the alert, the related personal data is 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.

E. 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 System has the right to request from Havas (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 France, under the French Data Protection Act, any person concerned by the alert has the right to define directives for the conservation, deletion and communication of their personal data after their death.

Any person concerned by the alert may exercise his or her rights by writing to the following e-mail address: dpo@havas.com, precisely setting out their request and enclosing proof of identity by any means.

In any case, any person concerned by the alert may refer to the competent data protection Authority, (in France, the French National Commission on Informatics and Liberty - (CNIL) for any claim or complaint concerning the processing of their personal data.

5

5. APPENDIX 2 - ARCHIVE RETENTION PERIODS

5. APPENDIX 2 - ARCHIVE RETENTION PERIODS

CATEGORIES OF REPORTED FACTS	ARCHIVE RETENTION PERIOD
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 ANTI-CORRUPTION	To be determined according to the applicable statutory limitation period based on the violation committed


HAVAS