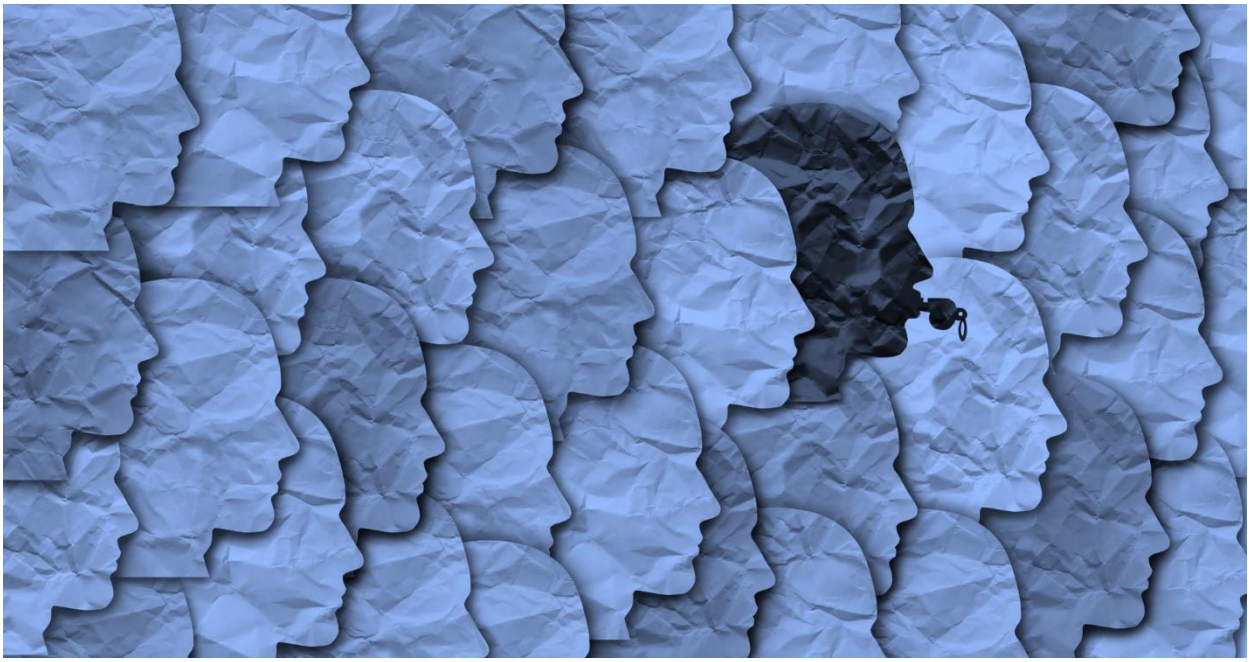
WHISTLEBLOWING

Collecting and handling alerts



BOLLORÉ

A BUSINESS ETHICS SHARED BY ALL

As part of its 2017-2022 Corporate Social Responsibility strategy, Bolloré is committed to unite its stakeholders around common ethical standards. This commitment is set out in a Code of conduct, binding upon its employees, business partners and everyone acting on behalf of the Group.

In the conduct of its business activities, the Group condemns corruption, influence peddling and anti-competitive practices. It ensures financial transparency, compliance with international sanction programs and the protection of personal data. It prevents damages to the environment, violations of human rights and fundamental freedoms, and risks to the health and safety of individuals. Lastly, it fights against all forms of discrimination and harassment.

The Bolloré Group enables its stakeholders, including its employees and business partners, to use this whistleblowing system to report behaviors contravening its Code of conduct or applicable laws. Awareness-raising initiatives about the system are deployed by the Group, together with the Code of Conduct about all of its components (compliance, duty of care, HR, etc.)..

Bolloré ensures the confidential processing of alerts and the protection of whistleblowers acting in good faith against any form of retaliation.

Perpetrators of misconducts, conclusive proof of which has been established through an adversarial process, face disciplinary actions or legal proceedings in accordance with applicable laws.

This procedure provides information relative to the purpose, conditions and guarantees of use of the whistleblowing system, the alert collection and handling process, and the protection of personal data. It has been submitted to employee representative bodies for consultation (in accordance with applicable laws).

For more information: compliance@bollore.com

Cyrille Bolloré
Chairman and Chief Executive Officer

MONITORING SHEET
approval circuit/update history

COMPLIANCE DEPARTMENT
BOLLORÉ GROUP

COMPLIANCE PROCEDURE Updated: 09/05/2022

WHISTLEBLOWING
Alert collection and handling procedure

REF: V2022.EN.1.0

Manager	Director	Validator
Compliance Department Human Resources Departmen CSR Departmentt	Gilles d'Arras David-Alexandre Fournier Elodie Le Rol – Berkmann	François Laroze

Changes compared with prior version	
› Adaptation to CNIL standard.	

CONTENTS

1. GLOSSARY

Whistleblower	Any person meeting the conditions set forth in article 2.1 reporting acts which fall within the scope of the system also described in article 2.1.
Implicated individuals	The perpetrator or perpetrators of the acts which fall within the scope of the system, together with any person implicated in such acts (including witnesses)
Coordinators	Persons appointed and authorised to receive alerts that fall within the scope of this system
Authorised third parties	Any third party appointed (by coordinators) to investigate all or some of the details of an alert

1. PURPOSE, CONDITIONS AND GUARANTEES OF USE

1.1. Purpose of the system

Bolloré's shared whistleblowing system is implemented by each of the companies making up the Bolloré group[1], alongside Bolloré SE. Its purpose is to meet the requirements for mandatory reporting systems provided by French Law for companies governed by it, as well as to receive reports violations of the Code of Conduct applicable to all companies of the group.

A shared accountability agreement has been entered into by the group's various companies. It contains clauses which are required by regulations related to personal data in order to ensure compliance with the obligations resulting from it for the people concerned.

Under the terms and conditions of this agreement, the relationships with the people concerned by such whistleblowing are mainly managed by Bolloré SE. As such, the people concerned are asked to contact Bolloré SE first should they need to do so, at the address given in article 4.2 below. Doing so will not affect their rights in relation to each person who is jointly responsible for handling their personal data.

This system enables people covered by it to bring acts which fall within its scope to the knowledge of all or some of these companies, the aim being to ensure that the reporting of these acts is handled effectively.

[1] The Bolloré Group operates in three main sectors: Transport and logistics, Communication and Electricity storage and systems. The Vivendi group has its own ethics system for managing its communication activities, applicable to its companies and adapted to their business lines.

The scope of this system is as follows:

Companies of the Bolloré Group covered by the whistleblowing system	Persons who may report	Acts which may be reported	Legal basis for processing of personal data
Mandatory component of the system			
Companies of the Bolloré Group of more than 50 employees	Employees or outside and occasional staff of one of these companies (interns, temporary workers, consultants, etc.)	Acts likely to constitute a crime or an offence (e.g.: discrimination, bullying over the telephone, workplace harassment or sexual harassment), serious and manifest violation of an international commitment that is regularly ratified or approved by France, of a unilateral act of an international organisation undertaken on the basis of such a commitment, of the law or regulation (e.g.: failure to comply with economic sanction programmes), or a threat or an act which may seriously jeopardise the general interest (e.g.: damage to the environment, threat to public health).	Legal requirements by which the companies concerned are bound (article 8 of law no. 2016-1691 of 9 December 2016 on transparency, tackling corruption and modernising economic life – known as the "Sapin II" law in France).

Parent company of Bolloré group + all its subsidiaries	Employees of companies bound by the obligation	Acts likely to constitute an act of corruption or of influence peddling	Legal requirements by which the companies concerned are bound (article 17 of law no. 2016-1691 of 9 December 2016 on transparency, tackling corruption and modernising economic life – known as the "Sapin II" law in France)

All limited companies or European companies of the Bolloré group which are: 1. head-quartered in France and have more than 5000 employees (internal + direct and indirect subsidiaries) 1. head-quartered in France or abroad and have more than 10,000 employees (internal + direct and indirect subsidiaries)	Any person	Information which can be used to identify risks and prevent serious violations of human rights and fundamental freedoms, or compromise the health and safety of people and the environment, resulting from the group's activities, as well as those of subcontractors or suppliers with which an established commercial relationship has been entered into, when these activities are associated with this relationship. A "serious violation" is any risk which might expose natural persons and the environment to effects the gravity of which will be determined on the basis of their scale, their scope and the extent to which these effects might be irremediable, in compliance with the provisions of article 14 of the UN's guiding principles on Business and human rights.	Legal requirements by which the companies concerned are bound (article L. 225-102-4 of the French commercial code, derived from the "duty of care" law)

Voluntary component of the system			
All companies not bound by above-listed obligations	Scope covered by article 8 of the Sapin II law above: • Employees of each company concerned • outside and occasional staff of each company concerned (interns, temporary workers, consultants, etc.) • Scope covered by article 17 of the Sapin II law above: • employees of each company Scope covered by the law on "duty of care": • any person Périmètre de la loi devoir de vigilance • toute personne	All acts which may be reported in application of the system's obligatory component.	Legitimate interest of the companies of the group, without prejudicing the interests of the people concerned, in having a single, clear system so that users can share details of acts which are in breach of French laws and which may harm the corporate interests of each one, as well as acts which are contrary to the Ethics codes which they have adopted, such that they may be effectively applied
All companies of the Bolloré Group	Anyone personally having knowledge of the facts	Behaviour or situations which are contrary to the Bolloré group's code of conduct, including corruption influence peddling, violation of human rights and fundamental freedoms,	

		threat to health and safety of people as well as the environment.	

1.1. Conditions for admissibility and garanties of use

Alerts are admissible only where they fulfil the following conditions :

- Authentication: the use of this system is limited to people listed in point 2.1, who must provide information such that they may be identified; By way of exception, anonymous reporting may be admissible, once examined in accordance with article 3.2 below, and provided the alert includes sufficient details for establishing the gravity of the related acts;
- Good faith: users of the system must act in a selflessly and in good faith; in this respect, the facts pertaining to the alert must be reported in an objective manner demonstrating their alleged nature.

In return, the user benefits from guarantees associated with the status of whistleblowers:

- Confidentiality: information that may lead to the identification of users are processed in a confidential manner by authorized persons and may only be disclosed with their prior consent, except to the judicial authority;
- Protection : this system is optional; it is not intended to substitute conventional methods for reporting acts covered by its purpose, but is instead intended to supplement them (particularly, regarding employees, line management). No disciplinary (or any other) action may be initiated for not using the system or for using it in good faith when – even if the acts reported are later proved to be inaccurate or do not give rise to any further action. However, individuals who use the system improperly may face disciplinary sanctions and legal proceedings.

2. PROCESS FOR COLLECTION AND HANDLING OF ALERTS

Alerts issued via the whistleblowing system (2.2) are subject to an analysis of their suitability (2.3) and, where applicable, an investigation (2.4) undertaken by specially authorized persons (2.1) aimed at establishing in a timely manner the materiality of the reported facts and justifying disciplinary measures taken against their perpetrators in accordance with applicable laws.

3.1. People specially authorised to handle alerts and data recipients

Alerts are received by coordinators according to their scope of responsibility. These coordinators are jointly appointed by all the companies of the group implementing the system – due to their position, expertise, authority and resources – for the purposes of analyzing the suitability of alerts and then undertaking or coordinating the ensuing investigation. All coordinators are bound by enhanced confidentiality obligations. They undergo training the alert system and the facts which fall within its scope.

Each coordinator is supported by a team made of a limited number of individuals employed by Bolloré SE, specially authorized to carry out the related missions and bound by the same obligations as the coordinator – including enhanced confidentiality and training.

The members of this team are selected based on their expertise in the areas in which the coordinator operates. They are part of the :

- Compliance Department, particularly for acts of corruption, influence peddling, anti-competitive practices, violation of an international engagement that has been ratified or approved by France, economic sanction programmes;
- Human Resources Department, particularly for acts of discrimination and moral or sexual harassment, threat to health and safety of individuals, human rights and fundamental freedoms involving an employee of a Bolloré Group company;
- Corporate Social Responsibility Department, particularly for acts of discrimination and moral or sexual harassment, damage to the environment, to people's health and safety, violations of human rights and fundamental freedoms or threats and serious damage to the general interest.

Alerts that do not fall into any of the categories listed above will be handled with the support of one of the coordinator's team members from the Compliance Department.

Coordinators and their team may be supported by authorized third parties, appointed by the coordinator based on their expertise and / or their impartiality. Such third parties may include lawyers, experts and auditors, provided they grant appropriate protection of personal data and are personally bound by Law or contract under the terms of which they must abide by strict confidentiality obligations.

The personal data of people concerned by an alert will be shared with Bolloré SE and may be shared with other entities of the Bolloré group (the one targeted by the investigation as well as any other company which is potentially concerned), if the analysis of the alert reveals it necessary to do so. Due to the Bolloré group's international presence, some data may therefore be sent outside the European Economic Area (EEA). This including countries which do not necessarily have personal data protection laws equivalent to the ones in force in the EEA. These transfers are either required for the acknowledgement, exercise or defence of rights before courts, or are made on a one-off basis and only to a limited number of people, and only provided that no other means exist to fulfil the obligation of the companies of the Bolloré group which are compelled by the law or in application of its own commitments to tackle the acts and violations that fall within the scope of this system.

The data making up the alerts is made accessible to certain service providers or data processors as defined in the regulations on personal data, responsible for the computer resources used within the framework of the system. The service providers are contractually bound to adhere to certain specific obligations, such that they will only use the personal data to which they have access in accordance with the instructions given by the companies in the group which use the system.

2.2. Alert collection

Alternatively to conventional channels for escalating information (such as line management), acts allegedly falling within the scope described in point 2.1 may be reported using the Bolloré group's whistleblowing system which can be accessed from the Bolloré group's websites and from those of its subsidiaries, or from any web browser via the following address:

Users of the system are asked to identify themselves and to complete in good faith a form describing as objectively, factually and exhaustively as possible the alleged misconducts of which they have become personally aware, in addition to the identity of those responsible and any other person involved, accompanied by any supporting documentation that can be used to gauge the suitability of the alert and then take action.

The data deemed essential for the purposes of handling the alert is marked on the collection form (usually with an asterisk). The whistleblower's attention is drawn to the fact that, except in the event of such data being genuinely essential for establishing the veracity of facts which may result in legal proceedings, no sensitive data such as described in article 4.1 below must be entered into the system.

Once the information has been collected ("submit the alert"), the system automatically generates a username and a password. The user requires this information to access the follow-up area on the website where they are able to delete, change or add information to their alert and track the progress in processing it.

The alert is instantly received by the coordinator.

The coordinator informs the users that their alert has been received as soon as possible and then provides them with an estimate of the timeframe within which they can expect it to be processed, together with a reminder of the procedures available to them for engaging in discussion with the coordinator in the follow-up area.

Individuals allegedly involved are notified within a month from the alert, except when precautionary measures are adopted by the coordinator. They are reminded of their rights, and they are offered the option to submit their observations regarding the facts forming the basis of the alert. Notification does not compromise the confidentiality of the user's identity. Notification may be postponed until precautionary measures have been adopted, if the details of the matter reported require such measures to secure and safeguard the physical or digital data (information systems, servers, software, networks, correspondence, emails) and the IT equipment (laptop, mobile telephone, etc.) of the individuals allegedly involved.

3.3. Suitability analysis

Coordinators and their team undertake an analysis of the alert in order to determine whether or not it is admissible – i.e., whether or not it falls within the framework of the system described in article 2.1 and / or whether or not it meets the conditions set forth in article 2.2.

To gauge the admissibility of the alert, the coordinator may within a reasonable timeframe ask for further details via the alert system follow-up section.

If the users identified themselves, they will receive a notification by email, inviting them to log on to their follow-up section. If they have submitted their alert anonymously, they will need to log on regularly in order to view any request for clarification which may be issued. Otherwise, if the alert does not include enough detailed factual information, it will automatically be declared non-admissible.

Coordinators and their team may refer to the President of the CSR, Ethics and Compliance Committee to rule on the suitability of alerts about which there is uncertainty.

At the end of the analysis process, coordinators rule on the admissibility or inadmissibility of the alert.

3.4. Investigation

If the alert is deemed admissible, an investigation is conducted to ascertain the materiality of the facts and decide what action – if any – is to be taken.

Coordinators and their team carry out or coordinate the investigation aimed at establishing the materiality of the violations and determining the responsibility of the individuals allegedly involved.

This investigation may be conducted with the support of or – should the facts require complete outsourcing in order to guarantee the impartiality of those undertaking the investigation – by one or several authorized third parties.

As part of the investigation, coordinators and their team or the authorized third parties are entitled to:

- Collect and computer-process any data (accounting, banking, IT, etc.) that they deem relevant (excluding data the collection of which is prohibited and subject to their keeping the quantities of data to a minimum) concerning the company or companies in question, the whistleblower and the persons implicated;
- Conduct adversarial interviews in which the persons allegedly involved are able to respond to the accusations levelled at them;
- Question any person to collect any information serving to verify the accuracy of the alleged facts.

They keep records of all diligences undertaken throughout the investigation (legal and technical analysis of the facts, collection of evidence, discussions with various stakeholders, listening to witnesses, undertaking of assessments, etc.).

If the facts detailed in the alert mean that precautionary measures are required, they are implemented once the President of the CSR, Ethics & Compliance Committee has been consulted. The date on which individuals allegedly involved are informed that an investigation has begun is then postponed until such measures are effectively implemented.

Following the investigation, coordinators present their findings, conclusions and remediation proposals to the President of the CSR, Ethics & Compliance Committee.

The President of the CSR, Ethics & Compliance Committee approves the coordinator's report and either closes the process or convenes an extraordinary meeting of the CSR, Ethics &

Compliance Committee for the purposes of issuing a ruling and then closing the process.

2.5. Follow-up to the investigation

Once an alert has been handled, it must be closed in accordance with the conditions described below:

Reason for closure	Cause	Consequence	Personal data retention period in the active database	Personal data archiving period with restricted access
Manifest inadmissibility	The alert does not fall within the scope of the system described in article 2.1 and / or does not meet the conditions set forth in article 2.2.	Straightforward closure	Immediate deletion following closure.	N/A
Improper use of the system	The facts reported are not proven and the user issued the alert in bad faith, making improper use of the system.	Closure followed by initiation, if necessary, of disciplinary and / or legal proceedings if this improper use constitutes grounds for such proceedings.	Retention until the end of the procedure and the expiry of legal remedies, followed by deletion.	N/A

Inaccurate or insufficient information	The materiality of the facts and / or the responsibility of the person implicated cannot be sufficiently established, without the bad faith of the whistleblower being established.	Straightforward closure without follow-up (no disciplinary or legal proceedings, no remedies), without reservations.	Until two months following closure, then deletion.	N/A

		Or closure with reservations (in the event of dubious or sensitive facts, for example), together with – where appropriate – prevention or mitigation measures.	Two months following closure.	Archiving for 6 years or for the prescriptive period, of just the attachments to the file, without any identification data, in order to defend the interests of the whistleblower, the persons implicated and the data processors, or to enable discovery ongoing breaches to be recorded. Then deletion.
Proven facts	The materiality of the facts and the responsibility of all or some of the persons involved are established.	Closure of the alert procedure together with disciplinary and / or legal proceedings against the persons involved, if these incidents constitute grounds for such procedures.	Retention until the end of the procedure and the expiry of legal remedies, followed by deletion.	

	The materiality of the facts or the responsibility of all or some of the persons implicated are established.	Closure of the alert procedure, together with remedial measures (restructuring, implementation of new procedures, etc.), appropriate prevention or mitigation measures (field audit, dialogue with relevant stakeholders, corrective action plan)	Until the end of the period needed to implement appropriate remedial measures.	Archiving for 6 years or for the prescriptive period of the data, in order to defend the interests of the whistleblower, the persons implicated and the data processors, or to enable ascertainment of continuous offenses. Then deletion.

When deleting personal data, data that is strictly anonymous is extracted. This data is retained for a six years period for statistical purposes (examples include rendering information for the purposes of the duty of care, controls undertaken by the relevant authorities, etc.).

The whistleblower is informed of the closure of the procedure in the follow-up section. Individuals involved are informed by any means that enables them to acknowledge receipt, but without compromising the whistleblower's identity.

Use of the whistleblowing system and measures taken to prevent or rectify the breaches that it has served to identify are on the agendas of the ordinary and extraordinary meetings of the CSR, Ethics & Compliance Committee.

PROTECTION OF PERSONAL DATA AND RELATED RIGHTS

4.1. Personal data subject to or excluded from processing

As part of the whistleblowing system, categories of personal data listed below may be communicated by the whistleblower and by any other person involved in processing alerts, together with the persons implicated. Furthermore, the data in question may be subject to processing:

- Identity (title, first name, last name), position and contact details (phone number,

email address) of the whistleblower;
- Identity (title, first name, last name), position and contact details (phone number, email address) of the individuals allegedly involved. Identity (title, first name, last name), position and contact details (telephone number, email address) of the persons in collecting and processing alerts;
- Facts subject to the alert;
- Elements collected for the purposes of the investigation;
- Reports on checks conducted ;
- Follow-up to the alert.

The categories of data listed below may not be mentioned (otherwise the alert may be deemed inadmissible) and will only be stored in the system if they are absolutely necessary for the purposes of establishing the materiality of the facts reported which may give rise to legal proceedings:

- Offences, criminal convictions, security measures;
- Information about disciplinary proceedings;
- Assessments of the social difficulties of the persons;
- Racial or ethnic background ;
- Political opinions ;
- Religious or philosophical beliefs ;
- Union membership ;
- Sex life or sexual orientation;
- Health data ;
- Genetic data ;
- Biometric identification data (fingerprints, written signature, etc.).

Special precautions will be taken to ensure the confidentiality and security of this data.

4.2. Definition and exercise of rights related to personal data

Users of the system, individuals allegedly involved in misconducts, coordinators and any person processing alerts have the right to access and rectify any incorrect personal data held about them and, where provided for by regulations, oppose and delete certain personal data, limit its use or request its portability with a view to transferring it to a third party, and also (for people living in France) decide on the fate of their data after their death. It should be remembered that the company to which a request is submitted may refuse to grant certain requests in relation to some of these rights (particularly the right to deletion) on legitimate grounds, such as the need to defend their rights in the courts or the legal obligation to retain some data.

Companies of the Bolloré group implementing this system grant individuals allegedly involved the right to share their observations starting on the date that they are informed

that an alert has been submitted.

To exercise these rights, simply sends an email to ethicalert@bollore.net attaching any documents proving your identity and justifying the request. For any additional information or problems regarding the use of personal data, the data protection officer (DPO) of the company in question can be contacted at the address listed in the DPO directory. Should any unresolved problems remain, the competent oversight authority in France (CNIL – the national data watchdog) may be contacted.

BOLLORÉ

Tour Bolloré, 31-32, quai de Dion-Bouton
92811 Puteaux Cedex – France
Tél. : + 33 (0)1 46 96 44 33
Fax : + 33 (0)1 46 96 44 22
www.bollore.com