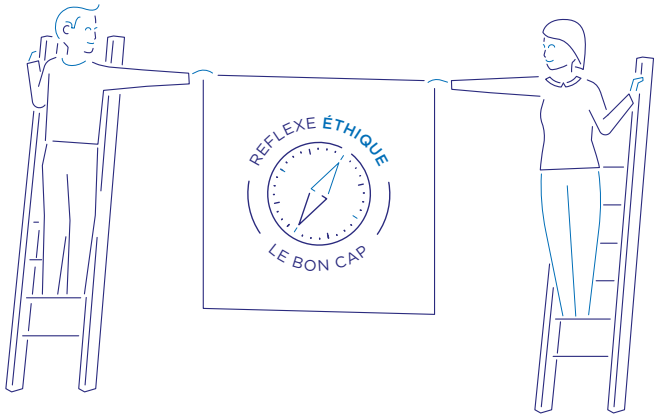
GROUPE ADP
SHARING NEW HORIZONS

CHARTER FOR THE PROCESSING OF ETHICS AND COMPLIANCE-RELATED ALERTS



The platform (https://alert.groupeadp.fr) is accessible 24/7
in the local language of the countries in which Groupe ADP operates.

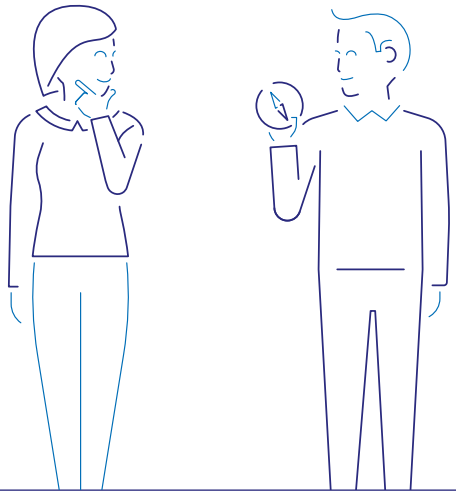
The platform is the primary channel for reporting an alert.

Alerts may be made anonymously in accordance with the rules of this Charter

Public Document - Before using this document, make sure you have the latest version of it.
Applicable from September 2023 _ Version 02 of 31/08/2023. Integrated printing of the ADP group - N°73710

SCOPE OF APPLICATION: ALL ADP GROUP EMPLOYEES

CONTENTS



INTRODUCTION

This Charter describes the whistleblowing system in place within Groupe ADP. It defines the **scope of application of the system, its operating procedures, the conditions of its use, and the retention of personal data** likely to be collected within the context of the system. It also describes the guarantees offered to protect people once an alert has been received.

In addition to accessibility, trust and confidence are prerequisites for the use and effectiveness of the whistleblowing system. The level of awareness of and trust in the system will be measured at least every two years by means of a Baromètre du Climat Éthique (Ethical Climate Survey).

The whistleblowing system is part of the Ethics and Compliance programme set up by Aéroports de Paris and rolled out across Groupe ADP. It is described in the Code of Conduct (appended to the Aéroports de Paris Internal Rules, which have been submitted to the Social and Economic Committee (SEC) for consultation. For subsidiaries, it is rolled out using the most appropriate local resources). Ethics and Compliance require every employee to behave in accordance with the law, regulations, internal rules and, more generally, the Group's values.

This system helps to protect employees and the company against the various risks to which they are exposed (human, financial, legal, reputational, etc.). It also helps them work together to defend the common good.

The purpose of the whistleblowing system is to collect internal alerts reported by Groupe ADP employees as well as external alerts reported by the entities mentioned in this document. It is also possible to report "externally", in accordance with the conditions laid down by Decree No. 2022-1284 of 3 October 2022, to one of the 45 authorities designated by this decree, to the judicial authority, or directly to the Défenseur des droits (French Citizens Rights Protector).

An alert may also be made public directly or referred to the judicial authorities in the event of imminent or obvious danger to the general interest, or when an internal or external alert cannot be effectively remedied or would expose the whistleblower to the risk of retaliation, as mentioned in Article 10-1 of the Sapin II Law, or due to the specific circumstances of the case, such as when evidence may be concealed or destroyed or when the whistleblower has genuine reason to believe that the authority may be in a conflict of interest or acting in collusion with the perpetrator of the violation or involved therein.

Alerts may relate to violations of the law or failure to comply with the provisions of the Group's Code of Conduct or, more generally, any breach relating to fundamental freedoms and human rights, the environment, or occupational health and safety.

The legal framework of the whistleblowing system is based on all laws of the countries in which the system is to be used, and in particular, as far as Europe and France are concerned, on:

- Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, which aims to improve the protection of whistleblowers and to create a common framework for protection within the European Union, transposed into two laws (Law No. 2002-401 of 21 March 2022 to improve the protection of whistleblowers and Organic Act No. 2022-400 of 21 March 2022 to strengthen the role of the Défenseur des droits in terms of whistleblowing), which led to the amendment of the Sapin II Law
- Law No. 2016-1691 of 9 December 2016 on transparency, the fight against corruption and the modernisation of economic life, known as the "Sapin II Law" (recognising the status of whistleblowers and the need to protect them)
- Implementing Decree No. 2022-1284 of 3 October 2022 for the implementation of the Waserman Law relating to the procedures for collecting and processing alerts made by whistleblowers and listing the external authorities instituted by Law No. 2022-401 of 21 March 2022 aimed at improving the protection of whistleblowers by defining what is considered to be retaliation
- Law No. 2017-399 of 27 March 2017 on the duty of vigilance of parent companies and contracting companies dealing with the environment and human rights.

THE 4 PILLARS OF THE WHISTLEBLOWING SYSTEM

- The protection of the whistleblower and the facilitators provided that they are acting in good faith in accordance with Article 6 of the Law of 9 December 2016
- Presumption of innocence of anyone targeted by an alert
- The proper conduct of the parties involved in the reception and processing of the alert
- Respect for the confidentiality of people and facts.

Any attempt to hinder or prevent someone from exercising their right to report an alert is a criminal offence (which can result in up to a year's imprisonment and a fine of €15,000.

1/ How should the whistleblowing system be used?

1.1. Definition of the whistleblowing system

The whistleblowing system set up within the framework defined above **constitutes an additional means of expression**, regardless of the whistleblowing channel used (platform, telephone, etc.) and independently of dialogue with managers or the HR network. It can be used by people inside or outside Groupe ADP who are authorised to report an alert, anonymously or otherwise.

Il It is used to:

- Make a request or ask a question relating to Ethics or Compliance, or seek help regarding a question or sensitive situation. Unless they result in an alert, questions are not considered to be admissible alerts. However, they must receive a response via the platform (if the alert is filed there) within a maximum of 3 months.
- Report facts concerning any of the fields falling within its scope of application.

1.2. Whistleblowing system stakeholders

The system is coordinated by the Group Ethics and Personal Data Division and in particular by the persons named in the appendix to this Charter. Only designated persons are authorised to access alerts in the whistleblowing platform. In certain cases and on their own initiative, they may grant certain access rights to the Ethics and Compliance Officers for matters that concern them, or to the Groupe ADP investigators.

The Ethics & Compliance Officers are the people named as the main contacts in the processing of alerts. In order to guarantee impartiality and the confidentiality of all those involved in processing the alerts, the Ethics & Compliance Officers must sign a confidentiality undertaking and apply the principles of this Charter. The Ethics and Compliance Officers at Hub One, AIG and TAV Airports (see appendix) may directly receive local alerts, in which case they must inform the Group's Ethics and Personal Data Division so that it can be input on the platform.

Managers who receive alerts must report them to the Ethics and Personal Data Division insofar as local law and confidentiality restrictions allow. To this end, guidance should be provided to managers so that they have clear instructions on how to deal with these alerts and when to report them.

The Human Resources Division must inform the Ethics and Personal Data Division of any alerts it receives, in accordance with the provisions defined between these two entities, in order to ensure, as far as possible, that alerts are properly processed.

The Ad Hoc Processing Committee is set up for each admissible alert. At the initiative of the Ethics and Personal Data Division, it will bring together a limited number of people with expertise in the field(s) relevant to the allegations (finance, legal, HR, etc.). These people will also sign a confidentiality undertaking.

1.3. Who can report an alert

Alerts can be made anonymously. To be admissible, anonymous alerts must include sufficiently detailed factual information and the serious nature of the facts must be established. In this case, the alert will be processed in the conventional manner.

The persons authorised to make a report (either via the platform or via the reporting channels provided for in this Charter) are:

- A natural person
- Members of staff on permanent or fixed-term contracts, interns, work-study students, former employees and job applicants when the information was obtained in the context of a former working relationship or job application
- External and occasional employees (temporary workers, agents and representatives, etc.)
- Shareholders and holders of voting rights at the entity's general meetings
- Members of administrative, management or supervisory bodies
- The entity's co-contractors and their subcontractors (suppliers, customers, etc.)

1.4. Alert reporting channels

There are various ways of contacting the Chief Ethics Officer, the Head of the Investigations Department, or their deputies: direct contact, by telephone or any other messaging service (voice, professional social network, etc.), by post, or via the alert platform in place within Groupe ADP.

The platform (https://alert.groupeadp.fr) is accessible 24/7 in the local language of the countries in which Groupe ADP operates.

Regardless of the channel is used, the alert must always be formalised via the dedicated platform. **Priority is to be given to this channel** in order to protect the whistleblower, the facilitators and any other individuals involved in the handling of the alert; it also enables the confidentiality of the information gathered and relevant conversations to be protected, and ensures that alerts are processed in the proper manner.

In the event that alerts are received by persons other than those named in this Charter, they must be forwarded without delay to the designated persons within the Ethics and Personal Data Division or the subsidiaries' Ethics and Compliance Officers.

1.5. Scope of application of the whistleblowing system

Information, facts or documents covered by medical confidentiality, legal professional privilege, national defence secrecy, the secrecy of judicial deliberations, the secrecy of a judicial investigation or the secrecy of a judicial inquiry **may not be disclosed in the alert**, at the risk of incurring civil and/or criminal liability.

Alerts may concern any breach of the Internal Rules (IR), to which the Code of Conduct or its equivalent in the subsidiaries is appended, the main principles of which are set out below:

- Compliance with laws and regulations
- Combating integrity violations
- Preventing corruption
- Conflicts of interest
- Preventing collusive and coercive practices and respecting the principles of free competition
- Prevention of influence peddling
- Gifts, invitations and other benefits
- Personal data protection
- Threats to or serious risks for the common good. For example, serious violations of human rights and fundamental freedoms, human health and safety and the environment
- Compliance with the principles of loyalty, fairness and integrity.

Alerts may also concern:

- A crime (e.g. aggravated theft, rape, terrorism) or another offence (tax fraud, falsification of accounts, corruption, misuse of company assets, breach of trust, illegal acquisition of interests, influence peddling, malicious phone calls or sending malicious messages, threats, sexual harassment or workplace bullying, discrimination of any kind, extortion, blackmail, fraud, illegal use of public funds, etc.)
- Violation or attempted concealment of a violation of an international commitment or European Union law
- Threat or harm to the common good or breach of a law or regulation.

2/ Rights and duties of stakeholders

2.1. General principlesx

All persons involved in the investigation of an alert are bound by a strict duty of confidentiality and must cooperate in the investigation of the alert.

To benefit from the protection granted to whistleblowers, the person submitting the alert must:

- Act in good faith (must reasonably believe that the facts reported are true at the time of their reporting)
- Make the disclosure or report without direct financial consideration
- Preserve the confidential nature of the alert made through the system.

Facilitators or certain individuals (family members, colleagues, etc.) who help the whistleblower report an alert will also benefit from the protection provided by law (in particular with regard to retaliation and psychological support measures).

Anyone who retaliates against a whistleblower or facilitator may be sentenced to 3 years' imprisonment and fined €45,000. No persons reporting or disclosing information may be subjected to any of the following measures, nor to threats or attempts to resort to such measures (the judge may award a provision for legal costs to a whistleblower who challenges a retaliatory measure or is subjected to a "gagging" procedure):

- Suspension, lay-off, dismissal or equivalent measures
- Demotion or denial of promotion
- Transfer of duties, change of workplace, reduction in salary, change in working hours
- Suspension of training
- Negative performance appraisal or work certificate
- Disciplinary measures imposed or administered, reprimand or other sanction, including a financial penalty
- Coercion, intimidation, harassment or ostracism
- Discrimination, disadvantageous or unfair treatment
- Non-conversion of a temporary employment contract into a permanent contract, where the worker could legitimately expect to be offered permanent employment
- Non-renewal or early termination of a temporary employment contract
- Damage, including to the person's reputation, particularly on social media, or financial loss, including loss of business and loss of income
- Blacklisting on the basis of a formal or informal agreement at sector or industry level, which may imply that the person will not find future employment in the sector or industry
- Early termination or cancellation of a contract for goods or services
- Cancellation of a licence or permit
- Referral for psychiatric or medical treatment

Any abusive use of the whistleblowing system (e.g. malicious accusations or defamation) will result in disciplinary action and proceedings against the offender. Persons engaging in dilatory practices (delaying the alert or the processing thereof) or abusive practices may be fined up to €60,000.

2.2. Commitment of the Alert Processing Committee

To ensure the proper implementation of the whistleblowing system, the members of the Processing Committee will observe the following commitments when performing their duties:

- Act **efficiently**, ensuring that they display **neutrality and impartiality** at all times. **A conflict of interest check will be carried out at each committee meeting**
- Gi**ve careful consideration to all alerts or requests** falling within the scope of the whistleblowing system
- **Be responsive** when it comes to acknowledging the alert and processing it
- **Inform** the whistleblower of the state of progress of the alert whilst also ensuring strict compliance with confidentiality rules
- **Protect** the parties involved, in accordance with the rules described below, **and in particular protect the confidential nature of the whistleblower's identity, the identity of the persons involved, and the associated information.**

All parties must sign a confidentiality undertaking reminding them of their obligations and the associated penalties. The Processing Committee is made up of only those people strictly needed to process the alert.

3/ The system's protection guarantees

3.1. Protection for whistleblowers and facilitators

All necessary precautions are taken by those involved in the whistleblowing process to guarantee the strict confidentiality of information likely to identify whistleblowers or facilitators, both when receiving the alert and when processing it.

The procedure must protect the integrity and confidentiality of the information received, "in particular the identity of the whistleblower, the persons concerned by the alert and any third party mentioned in the alert", and at the same time ensure that unauthorised persons cannot access the details of the alert. Third parties may only be privy to this information if it is needed to process the alert, in compliance with the conditions set out in Article 9-I of the Sapin II Law.

Information identifying the whistleblower may only be disclosed with the whistleblower's consent, except when it is disclosed to the judicial authority, in which case the whistleblower shall be notified as such, unless such information is likely to compromise the associated judicial proceedings.

When it is necessary to call upon third parties (e.g. a forensic firm) as part of the processing of the alert, the Ethics and Personal Data Division ensures that they are bound by the same duty of confidentiality as those involved in the whistleblowing system.

Any breach of confidentiality (identity, information, etc.) by those involved in the whistleblowing process or by any person authorised to process an alert may result in disciplinary or criminal penalties (under the Sapin II Law) of up to 2 years' imprisonment and a fine of €30,000. As a reminder, these persons have signed an undertaking in this respect.

Protection measures

When the persons concerned (whistleblowers and facilitators) exercise their right to use the whistleblowing system, retaliation of any kind (e.g. intimidation, damage to reputation, particularly on social media, etc.) is prohibited and punishable. If an individual feels they have been the victim of retaliation, they can report this to the Ethics and Personal Data Division via the platform.

Whistleblowers who remove, misappropriate or conceal confidential documents containing information relating to the alert will not be held criminally liable, provided that they had lawful access to them. These provisions also apply to accomplices to these offences. Whistleblowers are also exempt from civil liability for any damage resulting from their whistleblowing as long as they were acting in good faith.

When an alert or public disclosure has been made anonymously, the whistleblower will benefit from the same protection if his or her identity is subsequently revealed.

3.2. Protection for persons targeted by an alert

All necessary precautions are also taken by those involved in the whistleblowing process to ensure that any information likely to identify the persons targeted by an alert (identity, job role, contact details) remains strictly private and confidential.

It should be noted that the identity of the person implicated by an alert may only be disclosed, except to the judicial authorities, once it has been established that the alert is well-founded. In all cases, any information likely to identify the whistleblower must never be shared with the person targeted by the alert.

3.3. Witness protection

All necessary precautions are also taken by those involved in the whistleblowing process to guarantee the strict confidentiality of those who give evidence. Any information likely to identify the whistleblower must never be shared with them.

3.4. Processing of personal data

The system for reporting and processing whistleblowing alerts described in this Charter necessarily involves the processing of personal data, for which Aéroports de Paris acts as Data Controller.

Purpose and legal basis

The purpose of this processing is to enable questions and alerts to be received and processed. It is based on the legal obligations imposed on Aéroports de Paris (ADP SA) and the entities making up Groupe ADP. The data collected and stored is hosted securely in accordance with the ISSP (Information System Security Policy) in restricted-access areas and only authorised persons have access thereto. The whistleblowing system is recorded in ADP SA's register of processing activities and a Personal Data Protection Impact Assessment (PDPIA) has been carried out.

Data collected and processed

Whistleblowers are reminded that they must only communicate factual information directly related to the subject of their alert through the whistleblowing system.

The following personal data is processed through the whistleblowing system:

- Identity, job role and contact details of the whistleblower when they are provided (whistleblower and facilitators)
- Identity, job role and contact details of the person targeted by the alert when they are provided
- Identity, job role and contact details of the parties involved in receiving and processing the alert, including witnesses, when they are provided
- Facts reported
- Information gathered as part of the verification of facts reported

- Records of interviews and investigations/checks
- Alert follow-ups.

Data retention period

If the alert is declared inadmissible, the associated data archived (once anonymised) within a two month period, under the responsibility of the Ethics and Personal Data Division.

Admissible alerts

For the duration of the investigation, all data is anonymised (with the exception of documents collected as part of the investigation) and is stored in a secure location to which only the persons from the Ethics and Personal Data Division named in the appendix to this Charter have access.

Once the investigation has been closed (verifications or enquiries)

All information collected and not appended to the investigation report/document will be destroyed two months after the investigation has been closed. Anonymised documents to be retained will be archived two months after the closure of the investigation on the alert platform, in a secure location to which only the persons from the Ethics and Personal Data Division named in the appendix to this Charter have access.

The anonymised investigation report/document and the non-anonymised documents that make up the appendix will be archived in Aéroports de Paris' C@pe archiving system no later than **two months after the investigation has been closed. In order to meet the obligation to prove the processing of alerts, the documents archived after the investigation has been closed are kept for a period of 12 years.**

Data recipients and transfers

Only the persons from the Ethics and Personal Data Division named in the appendix to this Charter have access to the data stored in a secure location.

Personal data may be shared with third parties (e.g. forensic firms, law firms) when this is necessary to process the alert (receipt of alerts, investigation, legal expertise). These service providers enter into contracts with Aéroports de Paris SA under which they undertake to provide sufficient guarantees regarding the processing and security of the data entrusted to them.

In the event that personal data is likely to be transferred outside of the European Economic Area, Aéroports de Paris SA shall put in place guarantees to ensure a sufficient level of data protection, in particular by signing the European Commission's standard contractual clauses (a copy of which is available on request from informatique.libertes@adp.fr).

Individual rights

Any person whose information is used in the context of the alert, including the person(s) targeted by the alert, shall be notified **within one month** of the use of their data or **within a reasonable time frame** when such information is likely to compromise the needs of the investigation (for example, where there is a risk of destruction of evidence). In this case, the notification will be deferred and delivered as soon as the risk to the investigation has been eliminated. If precautionary measures need to be taken, the Processing Committee will arbitrate on the proportionality and necessity of such measures.

In accordance with the applicable legislation on Personal Data, the persons identified in the context of the whistleblowing system have a certain number of rights concerning the collection and processing of their personal data, namely:

- The right to access: individuals have the right to obtain (i) confirmation as to whether or not personal data relating to them is being processed and, if it is, to obtain (ii) access to and a copy of such data. The exercise of this right must not, however, violate the rights and freedoms of third parties or hinder the proper conduct of the investigation
- The right to object: when data is processed to enable Aéroports de Paris SA to comply with a legal obligation (e.g. Sapin II Law), the right to object is not applicable
- The right to rectify: individuals have the right to have inaccurate personal data rectified. They also have the right to have incomplete personal data completed, including by providing a supplementary declaration. This right must not, however, allow the data subject to retroactively modify information contained in the alert or collected as part of its investigation
- The right to restrict processing: in certain circumstances, individuals have the right to restrict the processing of their personal data
- The right to provide instructions concerning the use of data after their death: individuals may give Aéroports de Paris SA instructions concerning the use of their personal data after their death.

These rights may be exercised by contacting the Ethics and Personal Data Division or the Data Protection Officer by email at: informatique.libertes@adp.fr or by post to: Data Protection Officer - 1 rue de France - BP 81007 - 95 931 Roissy Charles de Gaulle Cedex - France.

If, after contacting the Data Protection Officer, data subjects consider that their rights have not been respected, they may file a complaint with the personal data protection authority.

4/ Processing whistleblowing alerts

4.1. Acknowledgement of receipt of an alert

Acknowledgement of receipt notifies the whistleblower that the alert has been received by the Ethics and Personal Data Division.

It is sent automatically via the platform (if the alert has been reported there) or within **7 working days** by the Ethics and Personal Data Division via email and informs the person who reported the alert that its admissibility will be examined in accordance with the procedure described below.

If the whistleblower so requests, a videoconference or physical meeting can be arranged to submit the alert. Such meetings must be held no later than 20 working days after receipt of the alert. Oral reports must be properly recorded (i.e. recorded on tape, transcribed or minutes taken). Similarly, the whistleblower must be able to check, rectify and approve the transcript or minutes, with records made of any changes and/or approval

4.2. Assessing admissibility

When an alert is received, the Ethics and Personal Data Division carries out a preliminary analysis to assess its admissibility. The purpose of this preliminary analysis is to determine whether the alert falls within the scope of application of the system, namely that:

- The whistleblower(s) meet the eligibility criteria
- The allegations fall within at least one scope of application of the system
- In some cases, the Ethics and Personal Data Division may request additional information, either to gain a better understanding of the scope of an alert or to be able to make a more accurate assessment of the alert's admissibility. In the latter case, if the whistleblower fails to respond, the alert will be deemed inadmissible. The plausibility of the facts reported

- The detailed nature of the facts reported or the items of evidence provided
- Compliance with the principles set out in this Charter.

The Ethics and Personal Data Division may decide to take precautionary measures even before the Processing Committee is set up, if it deems it necessary.

4.3. Notifying the admissibility of an alert

Within a period **of no more than three months** from the issue date of the acknowledgement of receipt of the alert (or, failing this, 3 months from the end of a period of 7 working days following the alert), the Ethics and Personal Data Division will notify the whistleblower of the admissibility of the alert, through the system described in this Charter. This notification will be provided in writing and will outline the measures planned or taken to assess the accuracy of the allegations and, where appropriate, to remedy the matter reported, as well as the reasons for these measures.

If the alert **is deemed inadmissible**, the Ethics and Personal Data Division will notify the whistleblower of the reasons for this negative decision and will advise them on what action will be taken (closure of the alert, transmission to another department for processing, etc.).

5/ Admissible alert processing procedure

5.1. Setting up an Ad Hoc Committee

Once an alert has been declared admissible, the Ethics and Personal Data Division analyses the information received to identify the various categories of allegations. If necessary, it may request additional information from the whistleblower or carry out preliminary checks to enable the Processing Committee to reach a decision on the nature of the processing to be carried out:

- Identification of any previous or parallel processing of the matter. For instance, actions already implemented by the HR network in response to a problem at work. In this case, the Ethics and Personal Data Division may decide whether it is necessary to continue the investigation initiated by the other department or to launch a parallel investigation
- Detailed description of the facts and identities of the people involved
- Identification of potential risks and/or conflicts of interest
- Etc.

The Ethics and Personal Data Division will set up an Ad Hoc Processing Committee made up of a limited number of people with expertise in the relevant field (finance, legal, HR, etc.), which will investigate the facts contained in the alert.

At the first meeting, the Processing Committee will carry out a formal check for potential conflicts of interest. Each member undertakes not to enter into a conflict of interest. In the event of a member declaring a conflict of interest, the other committee members will confirm how they wish to deal with it. This check is in addition to the due diligence performed upstream by the Ethics and Personal Data Division when analysing the alert.

The Committee meets as often as is necessary, notably to validate the processing strategy, to steer the progress of the alert processing, to arbitrate, and to validate any conclusions and recommendations. The Processing Committee may also decide to take precautionary measures.

5.2. Processing admissible alerts

Depending on the nature and severity of the facts reported, or the risks involved, the Ad Hoc Processing Committee may decide on the type of processing to carried out. This can take several forms.

Checks may be carried out by the Ethics and Personal Data Division, the Ethics and Compliance Officer, the internal investigation team or any other person appointed by the Processing Committee. These checks can either help to refute or confirm the allegations, or serve as a basis for other ways of processing the alert.

An internal or external audit or the monitoring of an existing audit.

An internal investigation which may be carried out by Groupe ADP's internal investigation team, or other parties (forensic firm, subsidiary officers, etc.), or a combination of several solutions. The Processing Committee will choose the solution most appropriate to the alert, taking into account a number of parameters (independence, specific expertise, scope of the investigation, etc.).

If the Committee initiates an investigation, its first report will constitute the investigation team's assignment order (when outside firms are called upon, the call for tenders won by the service provider will constitute the assignment order).

Or any other relevant action decided by the Processing Committee.

5.3. Closure of the alert processing procedure

The decision to end all operations relating to the processing of the alert will be taken by the Ad Hoc Processing Committee.

The whistleblower and the person targeted by the alert are notified in writing by the Ethics and Personal Data Division that the alert processing procedure has been closed. At the end of the investigation or checks, the Ethics and Personal Data Division may issue recommendations based on the conclusions of the investigation and the opinion of the Ad Hoc Processing Committee. These recommendations may relate to the individual case or to the Group's operations (procedures, processes, etc.).

The document formalising the recommendations issued by the Ethics and Data Protection Division is given to the relevant persons who must make the decisions relating to these recommendations in accordance with the opinion of the Processing Committee. The transmission of these recommendations marks the end of the investigation and therefore the closure of the procedure.

In the event of a recommendation for disciplinary action, the time limit for initiating the disciplinary procedure begins from the date on which the person authorised to initiate the procedure becomes aware of the wrongdoing (i.e. the date on which the document containing the recommendations is sent).

5.4. System monitoring

Each year, the Ethics and Personal Data Division produces a report on the actions implemented for the Audit and Risk Committee, the Board of Directors and the Executive Committee. As part of this process, it provides an update on the whistleblowing system via a statistical monitoring table which contains anonymised information and no personal data, ensuring that it cannot be traced back to an employee so as to protect his/her identity.

These actions may lead to the updating or early revision of the following:

- corruption risk mapping
- the Code of Conduct
- the Training plan

- ethics and compliance procedures
- internal alert processing procedures
- internal control procedures (accounting controls, ethical controls, etc.)
- the disciplinary system.

6/ Internal investigations

6.1. The principles of internal investigation

Investigations, whether conducted internally or externally, are governed by the rules contained in the document on the ethics of internal investigations and the following fundamental principles:

- Professionalism
- Respect for confidentiality
- Neutrality / impartiality
- Objectivity
- Respect for the presumption of innocence
- As a precautionary measure, the Ethics and Personal Data Division may decide to postpone informing the manager and employee affected by the alert, provided this is approved by the Processing Committee.

Alerts reporting cases of ill-treatment or harassment are processed in the same way as other alerts, but certain precautions are taken in view of the significant psychosocial risks that may arise in these situations.

In addition, if the alert is connected with a known or suspected psychosocial risk, the Ethics and Personal Data Division will alert the relevant persons or entities within the Group (occupational physician, person in charge of quality of life at work, etc.) directly or via the person deemed best placed to do so (e.g. manager), so that the risk can be dealt with while continuing to process the alert received.

The Ethics and Personal Data Division may take the necessary precautionary measures (without presuming the responsibilities of each party) in collaboration with the Human Resources Division in order to protect the whistleblower and/or the person targeted by the alert.

IN ALL CASES:

The **Ethics and Personal Data Division remains responsible for the processing of the alert and maintains a close relationship with the whistleblower.**

Although the investigations and audits performed following an alert may have serious professional or personal implications for the persons accused, **they may not under any circumstances be considered equivalent to a judicial enquiry or criminal investigation**. Upon completion of the investigation, the Ad Hoc Committee may forward the case to the judicial authorities in order for them to pursue it, in the event that the alert has demonstrated the existence of a criminal offence.

6.2. Cooperation of employees interviewed as part of an investigation

By virtue of the duty of loyalty inherent in their employment contract, employees interviewed as part of an investigation are required to cooperate and assist in these enquiries. To this end, they are expected to:

- sign the confidentiality undertaking provided to them
- attend interviews set up by the investigation team
- answer in good faith the questions asked by the investigation team
- provide any information requested by the investigation team that may be useful to the investigation.

Any behaviour or action likely to hinder investigations, in particular refusing to attend interviews or answer questions from the investigation team, providing misleading information or concealing information, is likely to lead the company to draw all the necessary legal conclusions.

7/ Appendices

Instructions for controlling information system use in the event of concerns regarding compliance with ethical rules and good information security practices

Please refer to the internal procedure (applicable only to ADP SA) on the intranet site: http://portail/sites/ethique_et_compliance or on request from the Group Ethics and Personal Data Division (stephanie.scouppe@adp.fr).

GROUPE ADP ETHICS AND COMPLIANCE NETWORK

AT GROUPE ADP LEVEL AND AT AÉROPORTS DE PARIS SA:		
People in charge of managing the whistleblowing system	**Stéphanie SCOUPPE** Chief Ethics Officer In her absence: **Isabelle CHIESA** Assistant to the Chief Ethics Officer	Mail : stephanie.scouppe@adp.fr Mail : isabelle.chiesa@adp.fr
	Nathalie VICTORY **Head of Investigations** In her absence: **Arnaud NICOLAS** Internal investigator	Mail : nathalie.victory@adp.fr Mail : arnaud.nicolas@adp.fr
The persons listed are also authorised to access the data collected and processed in relation to the alerts.		

At Airport International Group (AIG) - Amman - Jordan Airport:	
Hazem KHIRFAN Legal and Compliance Director AIG	Mail : Hazem.Khirfan@aig.aero

At TAV Airports:	
Can ALPTEKIN Head of Audit	Mail : Can.Alptekin@tav.aero

At Hub One:	
Olivier MELLINA-GOTTARDO Secretary General / Compliance Officer	Mail : olivier.mellina-gottardo@hubone.fr

The 10 rules of the whistleblowing system

1) The whistleblowing system has been set up in accordance with legal and regulatory provisions (the Sapin II and Potier laws) and the Code of Conduct appended to ADP SA's Internal Rules and their equivalents in the subsidiaries

2) The use of the whistleblowing system is not an obligation. It is a right that the people concerned may exercise freely

3) Alerts can be processed anonymously as long as the facts reported are sufficiently detailed and their severity has been established

4) A specific organisational system has been set up to receive and process alerts. The Ethics and Compliance Officers in charge of the whistleblowing system are subject to a strict duty of confidentiality with regard to the information they receive. Any breach of confidentiality is punishable by up to 2 years' imprisonment and a €30,000 fine

5) The Ethics and Compliance Officers in charge of processing the alert will acknowledge receipt within seven days of receiving the alert, and will determine its admissibility within a maximum period of three months

6) Whistleblowers shall incur no sanctions as long as they use this system in good faith and without direct financial compensation. The alert shall be kept confidential throughout the period of its processing, unless expressly agreed in advance. Whistleblowers and facilitators are protected from retaliation and may contact the Ethics and Personal Data Division directly or via the platform at any time

7) No person may, for reporting or disclosing information, be subjected to the following measures, nor to threats or attempts to resort to such measures: 1) Suspension, lay-off, dismissal or equivalent measures; 2) Demotion or denial of promotion; 3) Transfer of duties, change of workplace, reduction in salary, change in working hours; 4) Suspension of training; 5) Negative performance appraisal or work certificate; 6) Disciplinary measures imposed or administered, reprimand or other sanction, including a financial penalty; 7) Coercion, intimidation, harassment or ostracism; 8) Discrimination, disadvantageous or unfair treatment; 9) Non-conversion of a temporary employment contract into a permanent contract, where the worker could legitimately expect to be offered permanent employment; 10) Non-renewal or early termination of a temporary employment contract; 11) Damage, including to the person's reputation, particularly on social media, or financial loss, including loss of business and loss of income; 12) Blacklisting on the basis of a formal or informal agreement at sector or industry level, which may imply that the person will not find future employment in the sector or industry; 13) Early termination or cancellation of a contract for goods or services; 14) Cancellation of a licence or permit; 15) Referral for psychiatric or medical treatment

8) An intentionally false alert or an alert that reveals a collusion between the person issuing the alert and the person in question, may be sanctioned in accordance with the Internal Rules

9) The whistleblowing system complies with laws and regulations and with the French data protection law of 6 January 1978 as well as Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, the European Data Protection Regulation (GDPR)

10) Within the limits defined by applicable law, users of the system and any person affected by it have a number of rights regarding their personal data (right to access, rectify, erasure, object, restrict processing and provide post-mortem instructions) that they may exercise by contacting:

the Ethics and Personal Data Division:
isabelle.chiesa@adp.fr
ou stephanie.scouppe@adp.fr

or the Data Protection Officer email:
informatique.libertes@adp.fr

by post:
1 rue de France BP81007
95931 Roissy Charles de Gaulle Cedex

Internal Investigation Ethics

In accordance with the Charter for the processing of ethics and compliance-related alerts, the Ad Hoc Processing Committee set up by the Ethics and Personal Data Division may decide to conduct an internal investigation into an alert received through the system set up by Groupe ADP.

The purpose of this document is to specify the general principles governing internal investigations and applicable to the persons designated by the Ad Hoc Processing Committee to perform them, as well as to describe how these investigations are to be conducted.

The rules contained in this document will also apply to third party investigators or auditors appointed by the Ethics and Personal Data Division after consultation with the Processing Committee.

General principles governing internal investigations

Article I

The internal investigation performed in order to investigate an alert must not be considered as being equivalent to a criminal investigation. The people in charge of the internal investigation act in strict compliance with the applicable laws and regulations and with the company's rules, with which they must ensure that they are fully familiar at all times.

Article II

The internal investigation focuses on proven or presumed criminal acts, violations of the Internal Rules or equivalent, or the Code of Conduct, disclosed in the alert, and not on individuals.

Its purpose is to verify the reality of the facts contained in the alert, where necessary, to identify the presumed perpetrators and to collect the information required to initiate disciplinary and possibly criminal proceedings, and to recommend any measures to improve the Group's processes.

Article III

During their investigations and when reporting back on their work, the persons in charge of the internal investigation must observe the following principles: integrity, objectivity, neutrality, impartiality, confidentiality and the adversarial principle.

When necessary, the persons in charge of the internal investigation must withdraw from it when they consider that a conflict of interest exists due to their particular relationship with one of the people concerned by the investigation, or their involvement in the matter concerned.

Article IV

The privacy and rights of individuals are respected throughout the internal investigation.

The investigator shall refrain from using or disclosing, directly or indirectly, any information gathered in the course of his activities, outside the scope of the investigation.

The internal investigator shall not seek out or disclose information relating to an employee's personal, family or medical situation, unless this is essential to the conclusions of the investigation.

They must record this processing in the Group's register of personal data processing activities.

Conducting an internal investigation

Article V

The internal investigation will be conducted impartially, examining all incriminating and exonerating facts, by at least two people, in strict compliance with the presumption of innocence of the persons concerned.

The investigations are carried out based on factual and objective evidence, disregarding any convictions, personal impressions or rumours and any value judgements.

Article VI

The persons in charge of the internal investigation must notify the people they meet and/or interview of this fact (please see below).

In application of the heightened confidentiality obligations incumbent upon them during the processing of the alert, they are not required to provide any clarification or other information concerning the circumstances of their requests.

Article VII

The people in charge of the internal investigation have access to Groupe ADP's sites and entities, and to any information or information system which they need to consult in order to perform the mission assigned to them, with the exception of information covered by national defence secrecy obligations.

When accessing information systems, the established procedure and data entry methods must be strictly adhered to. They may request a copy of any documents considered useful to the investigation.

Article VIII

When required, the persons in charge of the internal investigation may interview people (witnesses, people targeted by the alert, or any other person considered useful) to obtain their explanations for the facts contained in the alert.

They may call upon an "investigative" lawyer, an "evidence collector", to carry out an internal investigation, either in response to an alert, or even when an investigation into the potential existence of illicit practices within the company is already underway by an administrative or judicial authority.

During these interviews, no pressure, threats or intimidation may be used against the interviewees.

The interviews are conducted by two people and will always result in an interview report drafted by the persons leading the interview and approved by the person being interviewed.

Article IX

All actions taken as part of the internal investigation to gather evidence must comply with strict rules designed to ensure the protection of individuals.

Notification of findings

Article X

The findings from the internal investigation will be the subject of a report which should be drafted in such a way as to ensure that it does not contain any information likely to identify the whistleblower.

This report must be approved by the Ad Hoc Processing Committee set up by the Ethics and Personal Data Division.

If the results of the internal investigation have made it possible to refute the facts stated in the alert, all of the information and data collected must be deleted in compliance with the Charter for the processing of ethics and compliance-related alerts.