APPENDIX TO THE INTERNAL RULES FOR ESCP Europe EMPLOYEES

WHISTLEBLOWER PROCEDURE

I. PURPOSE AND SCOPE OF THE WHISTLEBLOWER PROCEDURE

The whistleblower procedure applies to the entire ESCP Group. Aimed at collecting and processing reports, it is the same for all ESCP entities and campuses abroad (Paris, London, Berlin, Turin and Madrid). However, this procedure may be adapted according to local specificities detailed in the appendix, in accordance with national laws implementing the European directive.

The Compliance Officer, made up of the Legal and Compliance Director and the ESCP Compliance Manager, supervises this procedure. ESCP is committed to strictly comply with the regulations and the compliance principles applicable to its activities. Compliance with ethical and regulatory standards is an obligation for all stakeholders and must be demonstrated at every organisational level. The creation of a culture of transparency is essential for the detection, monitoring, and disposal of any illegal behaviour.

The whistleblower procedure is a unique tool designed to collect **two types of alert**:

(1) On the one hand, 'GENERAL' WARNINGS

The areas likely to be affected by these general warnings are as follows:

- **Discrimination / Harassment / Sexist or sexual violence.**
- **Health, hygiene, and safety at work.**
- **Protection of the environment.**
- **Accounting, finance, banking.**
- **Protection of personal data (GDPR).**

The following persons can issue a 'General' warning to ESCP:

- ESCP employees, former employees, and prospective employees.
- shareholders, members, and holders of voting rights at the General Meeting.
- members of the administrative, management or supervisory bodies.
- external or occasional employees: employees on secondment or temporary staff, trainees, agents, and representatives, etc.
- co-contractors (service providers, suppliers, customers, etc.), their sub-contractors or, in the case of legal entities, members of the administrative, management or supervisory bodies of these co-contractors and sub-contractors, as well as members of their staff.

In particular, ESCP provides that the Whistleblower Procedure is open to the ESCP Learning Community following the Initial Training and Executive Education programmes. This procedure does not supersede and complements **the specific 'Inclusion and Diversity' procedure** included in ESCP's internal rules relating to reports received by the learning community concerning discrimination and sexual and gender-based violence. As soon as a report falling within the remit of the Diversity Committee is received, it is referred to the Committee, which takes charge of the investigation.

(2) On the other hand, ANTI-CORRUPTION ALERTS concerning situations likely to constitute **corruption or influence peddling and contrary to the ESCP Code of Conduct**.

The reporting of anti-corruption warnings **is open to the following persons**:

- ESCP staff members;
- external or occasional employees: employees on secondment or temporary staff, trainees, agents and representatives employed by subcontracting companies

II. PERSONS ENTITLED TO WHISTLEBLOWER PROTECTION STATUS

1. The whistleblower, author of the alert

Whistleblowers can benefit from the protective status provided for by law as soon as the following criteria are met:

- The whistleblower must be a **natural person**,
- Who **reports or discloses information obtained during their professional activities**,
- **Related to** a crime, an offence, a threat or harm to the public interest, a violation or an attempt to conceal a violation of an international commitment duly ratified or approved by local legislation, a unilateral act of an international organisation taken on the basis of such a commitment, European Union law, or a law or regulation,
- **Without direct financial consideration and in good faith.**

NB: If the information was not obtained during their professional activities, the whistleblower must, in addition to these conditions, have personal knowledge of the facts in order to report them, which rules out the reporting of suppositions or hearsay. However, the whistleblower may only report these specific facts via the external channel.

2. The whistleblower's entourage

The following persons are also eligible for whistleblower protection:

- **Facilitators**: i.e. any natural or legal person under private non-profit law who helps a whistleblower to make a report (e.g. associations, trade unions).
- **Individuals in a relationship with a whistleblower** who are at risk of retaliation during their professional activities by their employer, their client or the recipient of their services (for example: colleagues and relatives of the whistleblower).
- **Legal entities controlled by** a whistleblower, for which he or she works or with which he or she has a professional relationship.

III. EXISTING REPORTING PROCEDURES: 3 SEPARATE ALERT CHANNELS

There are three channels available to whistleblowers: **INTERNAL, EXTERNAL AND PUBLIC DISCLOSURE.**

- Initially, the person issuing the alert can choose to:
  - Send an **internal alert**, if they have become aware of the information concerned during their professional activities, or
  - Send an **external alert**, after using the internal alert channel or directly.

- The author of the alert is also entitled to make a **public disclosure**, under certain conditions, in particular after having issued an external alert.

Whistleblowers will benefit from **the protection afforded by law** if they comply with the conditions set out below for the use of each of these channels:

1. The internal channel (internal reporting procedure)

a. For general alerts: the following individuals may use the internal channel:

- members of staff, former members of staff and applicants for employment.
- shareholders, members, directors, and holders of voting rights at the General Meeting.
- members of the administrative, management or supervisory bodies.
- external or occasional employees (employees on secondment or temporary staff, trainees, agents, and representatives, etc.).
- ESCP's co-contractors (service providers, suppliers, customers, etc.), their sub-contractors or, in the case of legal entities, members of the administrative, management or supervisory bodies of these co-contractors and sub-contractors, as well as members of their staff.
  In particular, the Internal Channel Alert System is open to the ESCP Learning Community following the Initial Training and Executive Education programmes.

b. For anti-corruption reports: the Alert System is only open to the following persons:

- ESCP staff members.
- external or occasional employees: employees on secondment or temporary staff, trainees, agents, and representatives employed by subcontracting companies, etc.).

2. External channel

This is a reporting procedure external to ESCP, to the competent authorities.

The author of the alert may, either after having sent an internal alert in accordance with the procedures described above, or directly**,** send an external alert to:

a) the competent authority, among those designated by implementing decree no. 2022-1284 of 3 October 2022 (see **attached** list)
b) the *'Défenseur des droits'*, who will refer the matter to the authority or authorities best placed to deal with it, or when an external authority does not consider itself competent.
c) The Judicial authority ;
d) An institution, body, office or agency of the European Union competent to collect information on breaches falling within the scope of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019.

Throughout the process, the person making the report will be able to benefit from the support of the new Deputy Ombudsman responsible for whistleblowers (https://www.defenseurdesdroits.fr/fr/lanceurs-dalerte).

Whistleblowers will thus be able to ask the *'Défenseur des droits'* to certify their status as whistleblowers, which will give them easier access to various protection measures against reprisals and gagging procedures, as well as privileged access to financial support schemes if their financial situation has seriously deteriorated because of the whistleblowing.

3. Public Disclosure

3.1. The author of the alert may **disclose information publicly** if one of the three following conditions is met:

a) **after having issued an external warning**, whether or not preceded by an internal warning, and **no appropriate action was taken** in response to this alert by the end of a period of three months from the date of acknowledgement of receipt of the warning; this period may be extended to 6 months on justification by the competent authority if the particular circumstances of the case (nature/complexity) require further action to be taken; **OR**

b) in the event of **serious and imminent danger**; OR

c) if referring the matter to one of the competent authorities referred to in III.2 above would entail a **risk of reprisals** or would **not make it possible to remedy the matter effectively**, because of the particular circumstances of the case, in particular if evidence could be concealed or destroyed or if the author of the alert has serious grounds for believing that the authority may have a conflict of interest, be in collusion with the perpetrator of the facts or be implicated in these facts.

3.2. By way of derogation from 3.1 b above, the whistleblower may, even in the absence of serious and imminent danger, publicly disclose information obtained in the course of his/her professional activities in the event of imminent or obvious danger to the general interest, in particular where there is an emergency situation or a risk of irreversible harm.

I.3. It is specified that Articles III 3.1 b, III 3.1 c and III 3.2 above do not apply where public disclosure would harm the interests of national defence and security.

IV. THE INTERNAL WHISTLEBLOWER PROCEDURE SPECIFIC TO ESCP

ESCP invites the whistleblower to use the internal channel to send his report.
This will guarantee the anonymity and confidentiality of the report and will enable ESCP to deal with the situation rapidly by means of a dedicated team depending on the type of report and to take any necessary disciplinary corrective action.

In addition, the whistleblower and those close to him/her (*as defined in article I.2 of these Rules*) shall benefit from the protection and guarantees set out in article II of these Rules.

1. Collecting internal alerts

1.1 How to receive an alert

All reports can be made to the Reporting Officer via several channels:

- Preferably directly on the **INTERNAL ALERT PLATFORM set up by ESCP,** at the following address: https://escp.signalement.net/entreprises

- Or by contacting the Coordinator **by EMAIL.**

1.2 Receipt of an internal alert by the Coordinator

All reports must be **brought to the attention of the Coordinator or, failing that, to the employer's line manager, who will pass them on to the Coordinator.**

The Coordinator is responsible for the following tasks:
- Collecting the reports they receive.
- **Acknowledging receipt of** the alert within **seven (7) working days** and informing the whistleblower of the way in which he/she will be kept informed of the follow-up to his/her alert.
- Drafting the communications/information to be sent to the whistleblower and to the persons concerned by the alert.
- Ensuring that alerts are dealt with in a timely manner.
- Taking any necessary interim measures.
- Informing the whistleblower and the persons concerned by the alert of the action taken.
- Guaranteeing the strict confidentiality of the identity of the whistleblower and the persons concerned, as well as the facts reported.

1.3 Content and admissibility of the alert

- **Identity / Anonymity**

The whistleblower can disclose their identity and functions if they so wish.

However, the present whistleblower procedure allows the whistleblower to **remain anonymous if they so wish.**

Information identifying the whistleblower **may only be disclosed with the whistleblower's consent**. It may, however, be communicated to the judicial authorities when required by law. The whistleblower is then informed, unless this information could compromise the legal proceedings.

- **The facts covered by the alert**

The information that can be reported must comply with the following conditions, otherwise it will be inadmissible:

- The information must relate to **certain specific offences** (listed in article III.1.b. hereof)

- The information must have been **obtained during professional activities at ESCP** and relate to facts that have occurred, or are very likely to occur, at ESCP.

- **The whistleblower must not receive any direct financial compensation and must be acting in good faith**. (NB: an alert issued in bad faith may consist of an excessive number of alerts).

- **The alert may not concern information** covered by national defence secrecy, medical secrecy, the secrecy of judicial deliberations, the secrecy of investigations or judicial enquiries, or legal privilege of lawyers.

- **Evidence**

Whistleblowers are invited to provide all information and supporting documents to substantiate their reports.

- **Acknowledgement of receipt of alert**

Within **seven (7) working days**, the Coordinator will inform the whistleblower that it has been received and of the deadline for examining the admissibility of the alert.

- **Examination of the admissibility of the alert**

The time limit for examining the admissibility of the alert is set at a maximum of two (2) months.

The admissibility check ensures that:
- The whistleblower and the facts reported fall within the scope of this procedure (limited to the areas concerned) and comply with the conditions defined above.
- The alert is reasonably well-founded and substantiated.

On receipt of an alert, the Coordinator:
- analyses the seriousness of the alleged facts and the *prima facie* admissibility of the warning.
- carries out basic checks where necessary. For example, it may ask the person who issued the alert for further details or additional documents.

At the end of this stage, there are two possibilities:

- Either the alert is declared INADMISSIBLE:
  - For a lack of information.
  - Because it does not fall within the scope of the present Arrangement.

NB: For instance, an alert is not inadmissible:

- It should be noted that the line manager of the person making the report may not under any circumstances be a member of the Compliance Committee, even if he or she is the subject of the report, without prejudice to respect for the rights of individuals.

In the event of particular difficulties (importance of the subject, persons involved, etc.) and for the purposes of the investigation, the report may be forwarded to the Chairman of the ESCP Audit Committee (or to the Chairman of the ESCP EESC who will succeed him if the Chairman of the Audit Committee is involved) by the Compliance Officer or a member of the General Management Committee in order to modify the persons involved in the Compliance Committee.

The Compliance Committee lists the actions to be taken and initiates an internal investigation to determine the reality and materiality of the facts reported and to remedy the situation.

If necessary, the Committee may also appoint a specialised *ad hoc* committee (which may be an existing committee or members of an existing department), which will submit regular reports to the Committee and carry out specific tasks as determined by the Compliance Committee. The latter is required to report periodically to the Compliance Committee and to carry out specific tasks, as explicitly defined by the latter, with a view to achieving these objectives:

1- Assess the accuracy of the facts :

- Search for evidence,

- Conducting interviews/hearings and drafting reports on respondents and witnesses,

- Search for IT items (email, documents, etc.)

2- Remedy/ Put an end to the incidents reported

To this end, Management provides the Compliance Committee with the resources it needs to gather and archive evidence.

Where appropriate, discussions may be organised with the whistleblower to ensure that his or her identity remains confidential.

In the event of hearings, the person(s) will be notified by email/through the platform at least seven (7) days in advance.

The members of the Compliance Committee will interview the person(s) named in the alert, who have been informed in advance that they have been implicated and of the facts of which they are accused. If he or she so wishes, the person implicated may be assisted by in-house counsel during these hearings.

The members of the Compliance Committee shall send the minutes of the hearings to the persons concerned for review, amendment if necessary, and validation.

The members of the Compliance Committee undertake to organise internal meetings between themselves to discuss ongoing issues.

Meetings can be held face-to-face or by videoconference.

Each member of the Compliance Committee has one vote. The members of the Compliance Committee deliberate by a show of hands or by secret ballot at the express request of one of the members. Decisions are taken by a simple majority.

At the end of the investigation, an **investigation report** presenting the conclusions of the investigations **and marking the closure of the investigation will be sent to the Chairman of the EESC ESCP Europe Audit Committee and** his representative on the campus appointed to decide on the action to be taken in response to any breaches found.

- **The Compliance Committee decides not to follow up the alert:**
  - It informs the whistleblower and the persons referred to in the alert in writing that the alert has been closed - no further action is taken on the alert.
    It is specified that it is not required to inform them of the reasons for closing the enquiry.
  - Within two months of the close of the investigation, it destroys all the information in the file that makes it possible to identify the author of the alert and the persons concerned by the alert.
  - After anonymisation, the file and the investigation report are archived. Archiving is carried out on a dedicated IT tool with restricted access.

- **The Compliance Committee decides that the investigation has been successful**:
  - It informs the whistleblower and the persons referred to in the alert in writing that the alert has been closed and that the investigation has been completed.
  - It archives all the data collected on a dedicated IT tool with restricted access, guaranteeing the confidentiality of the data recorded.
  - When disciplinary or litigation proceedings are initiated against a person implicated or the author of an abusive alert, the data relating to the alert is kept until the end of the proceedings or the time limit for appeals against the decision.

  In the event of an infringement:
  - The Compliance Committee may **take any useful measure at any time to put an end to the infringement**, in particular by contacting the person responsible for putting an end to it.
  - If no solution is found within ESCP to put an end to the infringement within a period of three months from the registration of the report, the Managing Director of ESCP or his local representative will transmit the information characterising the infringement to the competent judicial and/or administrative authority.

  If the investigation report establishes the existence of conduct or situations that contravene the internal regulations and its appendices, **the Executive Board decides on any disciplinary sanctions and/or legal proceedings against the persons involved.**

Once the Compliance Committee has dealt with the alert, whatever the outcome, the decision taken will be formalised in a document which will be sent (in whole or in part) to the whistleblower by the Compliance Officer.

If the investigation report establishes a breach by the whistleblower of his/her obligation to act in good faith or the slanderous nature of the alert, he/she will no longer benefit from the protection afforded by his/her status as a whistleblower. Consequently, the General Management will be informed and will then decide on any disciplinary action and/or legal proceedings to be taken against the whistleblower.

Where disciplinary proceedings or legal proceedings are initiated against the respondent or the perpetrator of an abusive alert, the data relating to the alert shall be kept until the end of the proceedings or the time limit for appeals against the decision.

VI. WHISTLEBLOWER PROTECTION

1. Prohibition of reprisals / retaliatory measures against the whistleblower

A whistleblower who has acted *in good faith and without direct financial consideration* may not be subject to any form of discrimination, dismissal, disciplinary sanction, or reprisal based on the right to blow the whistle in accordance with this procedure.

Any act or decision taken in disregard of these rules is therefore automatically null and void.

2. Civil and criminal liability of whistleblowers

Whistleblowers who have reported or publicly disclosed information under the conditions laid down shall not be civilly liable for damage caused by their reporting or public disclosure if they had reasonable grounds for believing, when they did so, that the reporting or public disclosure of all the information was necessary to protect the interests in question.

Whistleblowers are also protected if they report facts that could be classified as a crime or offence.

The facts may relate to "information" about a crime, an offence or violations of the law, but also to "attempts to conceal" these violations. As a result, the violation of the rule does not have to be "serious and manifest" in order to be reported.

VII. CONFIDENTIALITY

The procedure for collecting and handling alerts guarantees the strict confidentiality of the identity of the whistleblower and of any evidence communicated/discovered during the internal investigation. Only the persons directly responsible for the internal investigation and/or those directly involved in deciding on the action to be taken in response to the alert may have access to the information processed as part of the alert.

Information identifying the whistleblower may only be disclosed with his/her consent, except to the judicial authority when the persons responsible for collecting and processing the alerts are required to report the facts to a judge. In this case, the whistleblower must be informed of this disclosure to the judicial authority, unless this information risks compromising the judicial proceedings.

Information identifying the person who is the subject of an alert may only be disclosed, except to the judicial authorities, once it has been established that the alert is well-founded.

VIII. PERSONAL DATA

"signalement.net" constitutes a means of processing of personal data implemented by ESCP (15 rue Armand Moisant, 75015 Paris), necessary to comply with a legal obligation within the meaning of c) of Article 6 of European Regulation (EU) 2016-679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data (the "General Data Protection Regulation" or "GDPR").

The purpose of "signalement.net" is to collect and process alerts relating to "general" diversity alerts and alerts relating to anti-corruption. It is also used for statistical purposes.

ESCP undertakes to process the personal data of any person identified in the context of an internal alert procedure, whether he or she is the whistleblower, is implicated or is referred to in the alert (facilitators, witnesses....), in compliance with the amended Act No. 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties, the RGPD and applicable local law. To this end, they **must be informed within 30 days** of the collection of their personal data.

The data collected in the context of this processing will be used only by the personnel within ESCP and the platform's administrators who are authorised to process reports, within the limits of their need to know.

Those affected have the right to access and restrict their personal data, in accordance with Articles 15 and 18 of the GDPR, and the right to have their data amended if it is inaccurate, incomplete, ambiguous or out of date, in accordance with Article 16 of the GDPR.

They may exercise these rights by sending a request accompanied by proof of identity to the ESCP DPO:

- Or by e-mail: dpo@escp.eu *;*

- Or by post: DPO / Service Juridique ESCP - 15 rue Armand Moisant - 75015 Paris

If you consider, even after lodging a complaint with ESCPs, that your personal data protection rights have not been respected, you may lodge a complaint with the CNIL at the following address: 3 Place de Fontenoy - TSA 80715 - 75334 Paris Cedex 07.

However, the person who is the subject of an alert may under no circumstances obtain information concerning the identity of the Author of the alert.

The data collected is stored as follows:

	TYPOLOGY	**SHELF LIFE** (*Subject to the legal obligations applicable to the retention of data and in particular to the statute of limitations corresponding to the facts complained of)*
GENERAL ALERTS **<u>Data processed</u>** - Details of the whistleblower (optional) : Identity details: surname, first name;	Discrimination / Harassment / Sexist and sexual violence	<u>Alert inadmissible :</u> Deletion of data without delay after closure of the procedure. <u>Alert deemed admissible :</u> The data is kept for one year after the alert is filed, before being anonymised. When disciplinary or litigation proceedings are initiated

Data relating to professional life: position, entity; Contact details: personal/business email, personal/business telephone number. - Factual information : Date and time; Location and context (free field); Description (free field); Frequency (free field); Indicators (open field); Evidence / testimony (free field); Steps taken (free field); Free attachments. - Details of the perpetrator, if any (optional) : Identity details: surname, first name; Data relating to professional life: position, entity; Contact details: personal/business email, personal/business telephone number;		against a person (natural or legal) who has been implicated or the author of an abusive alert, the data relating to the alert is kept until the end of the proceedings or the time limit for appeals against the decision.
	Health, hygiene and safety at work	<u>Alert inadmissible :</u> Deletion of data without delay after closure of the procedure. <u>Alert deemed admissible :</u> The data is kept for one year after the alert is filed, before being anonymised. When disciplinary or litigation proceedings are initiated against a person (natural or legal) implicated or the author of an abusive alert, the data relating to the alert is kept until the end of the proceedings or the limitation period for appeals against the decision.
	Protection of the environment	<u>Alert inadmissible :</u> Deletion of data without delay after closure of the procedure. <u>Alert deemed admissible :</u> The data is kept for one year after the alert is filed, before being anonymised. When disciplinary or litigation proceedings are initiated against a person (natural or legal) implicated or the author of an abusive alert, the data relating to the alert is kept until the end of the proceedings or the limitation period for appeals against the decision.
	Accounting, finance, banking	<u>Alert inadmissible :</u> Deletion of data without delay after closure of the procedure. <u>Alert deemed admissible :</u>

		The data is kept for one year after the alert is filed, before being anonymised. When disciplinary or litigation proceedings are initiated against a person (natural or legal) implicated or the author of an abusive alert, the data relating to the alert is kept until the end of the proceedings or the limitation period for appeals against the decision.
ANTI-CORRUPTION ALERTS **<u>Data processed</u>** - Data concerning the whistleblower : Data relating to professional life: status, entity ; Status: victim/witness/third party Identity details (optional): surname, first name Contact details (optional): telephone number, postal address - Factual information : Object (free field) Date / period Location (free field) Description (free field) Free attachments	Anti-corruption, influence peddling and other breaches of probity	Alert inadmissible : Removal within 2 months of treatment. Acceptable alert : The data is kept for one year after the alert is filed and after deletion. When disciplinary or litigation proceedings are initiated against a person (natural or legal) who has been implicated or the author of an abusive alert, the data relating to the alert is kept until the end of the proceedings or the time limit for appeals against the decision.

IX. APPENDICES

ANNEX 1: LIST OF EXTERNAL AUTHORITIES FOR ALERTS (BY DOMAIN) VIA THE EXTERNAL CHANNEL IN FRANCE

a. Public procurement :

- French Anti-Corruption Agency (AFA), for breaches of probity;
- Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF), for anti-competitive practices;
- Autorité de la concurrence, for anti-competitive practices ;

b. Financial services, products and markets and the prevention of money laundering and terrorist financing :

- Autorité des marchés financiers (AMF), for investment services providers and market infrastructures;
- Autorité de contrôle prudentiel et de résolution (ACPR), for credit institutions and insurance companies;

c. Product safety and conformity :

- Directorate-General for Competition, Consumer Affairs and Fraud Control (DGCCRF) ;
- Service central des armes et explosifs (SCAE) ;

d. Transport safety :

- Direction Générale de l'Aviation Civile (DGAC), for air transport safety;
- Land Transport Accident Investigation Bureau (BEA-TT), for land transport safety (road and rail);
- Directorate-General for Maritime Affairs, Fisheries and Aquaculture (DGAMPA), for maritime transport safety;

e. Environmental protection :

- General Inspectorate for the Environment and Sustainable Development (IGEDD) ;

f. Radiation protection and nuclear safety :

- French Nuclear Safety Authority (ASN) ;

g. Food safety :

- General Council for Food, Agriculture and Rural Areas (CGAAER) ;
- Agence nationale chargée de la sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES);

h. Public health :

- Agence nationale chargée de la sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES);
- National public health agency (Santé publique France, SpF);
- French National Authority for Health (HAS);
- Agence de la biomédecine ;
- French Blood Establishment (EFS);
- d'indemnisation des victimes des essais nucléaires (CIVEN) ;
- General Inspectorate of Social Affairs (IGAS) ;
- French National Institute for Health and Medical Research (INSERM) ;
- Conseil national de l'ordre des médecins, for the practice of the profession of doctor ;
- Conseil national de l'ordre des masseurs-kinésithérapeutes, for the practice of the profession of masseur-kinésithérapeute ;
- Conseil national de l'ordre des sages-femmes, for the practice of the profession of midwife;
- Conseil national de l'ordre des pharmaciens, for the practice of the profession of pharmacist ;
- Conseil national de l'ordre des infirmiers, for the practice of the profession of nurse; - Conseil national de l'ordre des chirurgiens-dentistes, for the practice of the profession of dental surgeon;
- Conseil national de l'ordre des pédicures-podologues, for the practice of the profession of chiropodist;
- Conseil national de l'ordre des vétérinaires, for the practice of the profession of veterinary surgeon ;

i. Consumer protection :

- Directorate-General for Competition, Consumer Affairs and Fraud Control (DGCCRF) ;

j. Protection of privacy and personal data, security of networks and information systems:

- Commission nationale de l'informatique et des libertés (CNIL) ;
- French National Agency for Information Systems Security (ANSSI) ;

k. Violations affecting the financial interests of the European Union :

- French Anti-Corruption Agency (AFA), for breaches of probity;
- Direction générale des finances publiques (DGFIP), for value added tax fraud;
- Direction générale des douanes et droits indirects (DGDDI), for fraud involving customs, anti-dumping and similar duties;

l. Infringements relating to the internal market :

- Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF), for anti-competitive practices;
- Competition Authority, for anti-competitive practices and state aid;
- Direction générale des finances publiques (DGFIP), for corporation tax fraud;

m. Activities conducted by the Ministry of Defence :

- General Control of the Armed Forces (CGA) ;
- College of Inspectors General of the Armed Forces ;

n. Public statistics :

- Public Statistics Authority (ASP) ;

o. Agriculture :

- General Council for Food, Agriculture and Rural Areas (CGAAER) ;

p. National education and higher education :

- Ombudsman for national education and higher education ;

q. Individual and collective labour relations, working conditions :

- Directorate-General for Labour (DGT) ;

r. Employment and vocational training :

- General Delegation for Employment and Vocational Training (DGEFP) ;

s. Culture :

- Conseil national de l'ordre des architectes, for the practice of architecture;
- Council of auction houses for public auctions ;

t. Rights and freedoms in relations with State administrations, local authorities, public establishments and bodies with a public service remit:

- Human Rights Defender ;

u. Best interests and rights of the child :

- Human Rights Defender ;

v. Discrimination :

- Human Rights Defender ;

w. Ethics of persons engaged in security activities :

- Human Rights Defender.