Whistleblowing Policy

Collection and processing of reports

June 2023

cve

Changing visions of energy

INTRODUCTION

In the course of its activities, CVE: prohibits any form of Corruption (including bribery, Influence Peddling and Favoritism);

prevents damage to the environment; promotes the health and safety of people, human rights, and fundamental freedoms; and proscribes discrimination and harassment of any kind.

CVE has adopted an **Ethics Charter** and an **Anti-Corruption Code of Conduct** (available on **www.cvegroup.com/en/our-commitments/).**

CVE has also implemented the present **Whistleblowing Policy,** whose objective is to allow a **Recipient** (as defined on page 4 (scope of application)), who has reasons to believe that any law, regulation, Policy, or internal CVE rule has been violated, to report it.

WHISTLEBLOWING POLICY

A **Recipient** will then be qualified as a whistleblower under French law as soon as he or she meets the following criteria:

> **"A whistleblower is a natural person who reports or discloses, without direct financial consideration and in good faith, information concerning a crime, an offense, a threat or harm to the general interest, a violation or an attempt to conceal the violation of an international agreement duly ratified or approved by France, of a unilateral act of an international organization taken on the basis of such a commitment, of the law of the European Union, of the law or of the regulations"[1].**

A Recipient may report facts to his or her supervisor (hereinafter the "Manager") or use the internal professional whistleblowing system, set up by CVE and described in this Whistleblowing Policy.

Reporting to the Manager or using CVE's internal professional alert system is optional.

Alternatively, Recipients based in France may address their reports to one of the competent French authorities listed in the appendix to this Policy.

[1] Article 6 of Law No. 2016-1691 of December 9, 2016 on transparency, the fight against Corruption and the modernization of economic life.

Scope of application

This Whistleblowing Policy applies to:

- all CVE entities, wherever they are located;
- all officers, shareholders, Employees (whoever they may be, including Employees, trainees, apprentices, temporary workers, etc., hereinafter collectively **"Employees"**), former Employees, job applicants of CVE Group companies, as well as all CVE business partners and members of their staff;
- whether these persons, whoever they may be, are in France or worldwide (hereinafter collectively **"the Recipients"**).

Report Recipient

The author of a report shall send the report to the Compliance Department in accordance with the procedures described in section 5 below by email to: **compliance-alert@cvegroup.com.**

The missions of the Compliance Department are carried out in an impartial manner.

Facts and behaviors that can be reported

A report may relate to the following situations:

- a violation of the Anti-Corruption Code of Conduct or the CVE Ethics Charter;
- any crime or misdemeanor;
- a violation or an attempt to conceal a violation of an international agreement regularly ratified or approved by France, of a unilateral act of an international organization taken on the basis of such a commitment, of the law of the European Union, of the law or of the regulations;
- a threat or harm to the general interest.

The **areas covered by the report** generally include, but are not limited to:

- harassment;
- Corruption/and Influence Peddling;
- Favoritism, illegal taking of interest or concealment of these offenses;
- irregularities in financial/stock market matters;
- serious violations of human rights — in particular, discrimination and infringements on equality, privacy, the right to strike, freedom of assembly and association, and fundamental freedoms;
- damage to the health and safety of people, such as sanitary risks and noncompliance with safe working conditions;
- discrimination;
- danger related to health, safety or hygiene at work, and damage to the environment.

À noter :

- the report may relate to events that have occurred but also to events that have not yet occurred but are very likely to occur;
- if the information on which the report is based was obtained in the course of his or her professional activities, the Recipient may report facts that have been reported to him/ her, in addition to those of which he or she has personal knowledge. On the other hand, if the report is based on information that he/she did not obtain in the course of his/her professional activities, the facts reported will be restricted to those of which he/she has personal knowledge.

Excluded from the scope of the report are facts, information or documents the revelation or disclosure of which is prohibited by:

- national defense secrecy;
- medical confidentiality;
- judicial deliberations secrecy;
- investigation or the judicial instruction secrecy;
- attorney-client privilege.

Filtering and preliminary analysis of report

1 - How to report

The report is sent by email to **compliance-alert@cvegroup.com**.

The report must include at least the following information:

- the identity, functions and contact details of the author of the report;
- the identity and functions of the subject(s) of the report (if this information is known);
- the description of the facts.

The author of a report must describe the facts and information of the report in an objective and precise manner.

The author of a report shall, as the case may be, provide documents or data to support the report.

2 - Anonymity

A report made by a person who wishes to remain anonymous can be processed if the following conditions are met:

- the seriousness of the facts mentioned is established;
- the factual elements are sufficiently detailed.

3 - Protection of the author of the report and his entourage

A Recipient who makes a report in good faith and without direct financial consideration, or refrains - except in specific cases required by law - from making such a report, whether or not using the internal reporting system, shall not suffer from any retaliation measures.

In addition, no disciplinary action or retaliatory action, directly or indirectly, will be taken as a result of a complaint, even if the facts are subsequently proven to be inaccurate or do not result in any action.

On the other hand, voluntary misuse of the whistleblowing system may expose the author of a report to disciplinary sanctions and/or legal proceedings.

The protection afforded to whistleblowers also applies:

- to facilitators, i.e., to any individual or any non-profit legal entity that helps an Recipient to report;
- to natural persons in connection with a Recipient;
- to legal entities controlled by a Recipient for which he/she works or with which he/she is in contact in a professional context.

Processing reports

The author of a report will be informed of the receipt of the report in writing within seven working days of its receipt.

He or she will then be informed, within a reasonable period of time not exceeding three months from the acknowledgement of receipt of the report, of the measures planned or taken to assess the accuracy of the allegations and, if necessary, remediation measures taken to address the wrongdoings.

All contact and communication (emails, telephone exchanges and physical meetings) will be secure. Exchanges may be recorded using means that ensure security and confidentiality and may be transcribed in whole or in part in a written report.

All information or evidence provided by the author of the report shall be examined to determine whether it is admissible in accordance (Cf. page 6, filtering and preliminary analysis of report).

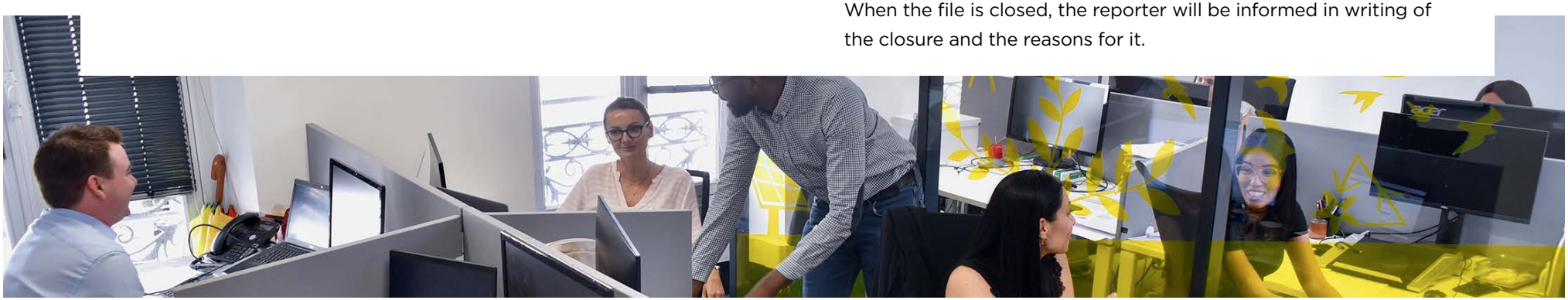
If the report is admissible, the Compliance Department will coordinate an investigation aimed at establishing the truthfulness of the facts and the materiality of the breaches, and characterizing the responsibility of the presumed perpetrator(s).

Procedure closure

In substance, the Procedure will be terminated on the following grounds:

- inadmissibility: If the analysis of the Compliance Department establishes that the report does not comply with the conditions described previously (in particular, with regard to anonymity), the Procedure will be closed without consequences to the author of the report;
- misuse of the system: If the analysis of admissibility or the ensuing investigation demonstrates bad faith by the author of the report the Procedure may be closed and disciplinary sanctions and/or legal proceedings taken against the author;
- incorrectness or inadequacy: If the investigation does not establish the truthfulness of the facts, the materiality of the breaches and the responsibility of the alleged perpetrator(s), and/or does not establish bad faith, the Procedure will be closed without consequences;
- materiality of the facts: If the investigation establishes the truthfulness of the facts, the materiality of the breaches and the responsibility of the presumed perpetrator(s), the Procedure will be closed and disciplinary sanctions and/or legal proceedings against the person(s) implicated will be initiated.

When the file is closed, the reporter will be informed in writing of the closure and the reasons for it.



Confidentiality

All information collected under this report system will be treated in strict **confidence,** whether it concerns the **identity of the author of the report,** the **alleged unethical/illegal actions** or the **persons to whom the report relates.** In addition, this confidentiality requirement is extended to the protection of the identity of **all third parties** mentioned in the report.

The persons in charge of collecting or processing reports are therefore subject to a confidentiality obligation.

Protection of personal data

1 - Purpose of the processing

The whistleblower system constitutes processing of personal data in accordance with the applicable laws and regulations regarding the protection of personal data.

The personal data collected within the framework of this system will be used by the data controller to meet legal obligations; the data that are essential from a regulatory point of view are indicated at the time of collection.

2 - Data controller

CVE, a French simplified joint-stock company with a capital of 48.499.236 euros, is registered in the Trade and Companies Register of Marseille under number 518792528 and acts as the controller of the personal data collected within the framework of the whistleblowing system.

3 - Categories of personal data

Categories of data collected at the time of the report and during verification of the report, as well as collection methods (e.g., alert reports), are limited to the following:

- identity, functions and contact details of the whistleblower;
- identity, functions and contact details of person(s) subject to a report;
- identity, functions and contact details of person(s) involved in the collection or handling of the report;
- reported facts;
- elements collected as part of the verification of reported facts;
- report on Audit Operations;
- follow-up to the report.

The facts collected are strictly limited to the areas covered by the reporting system.

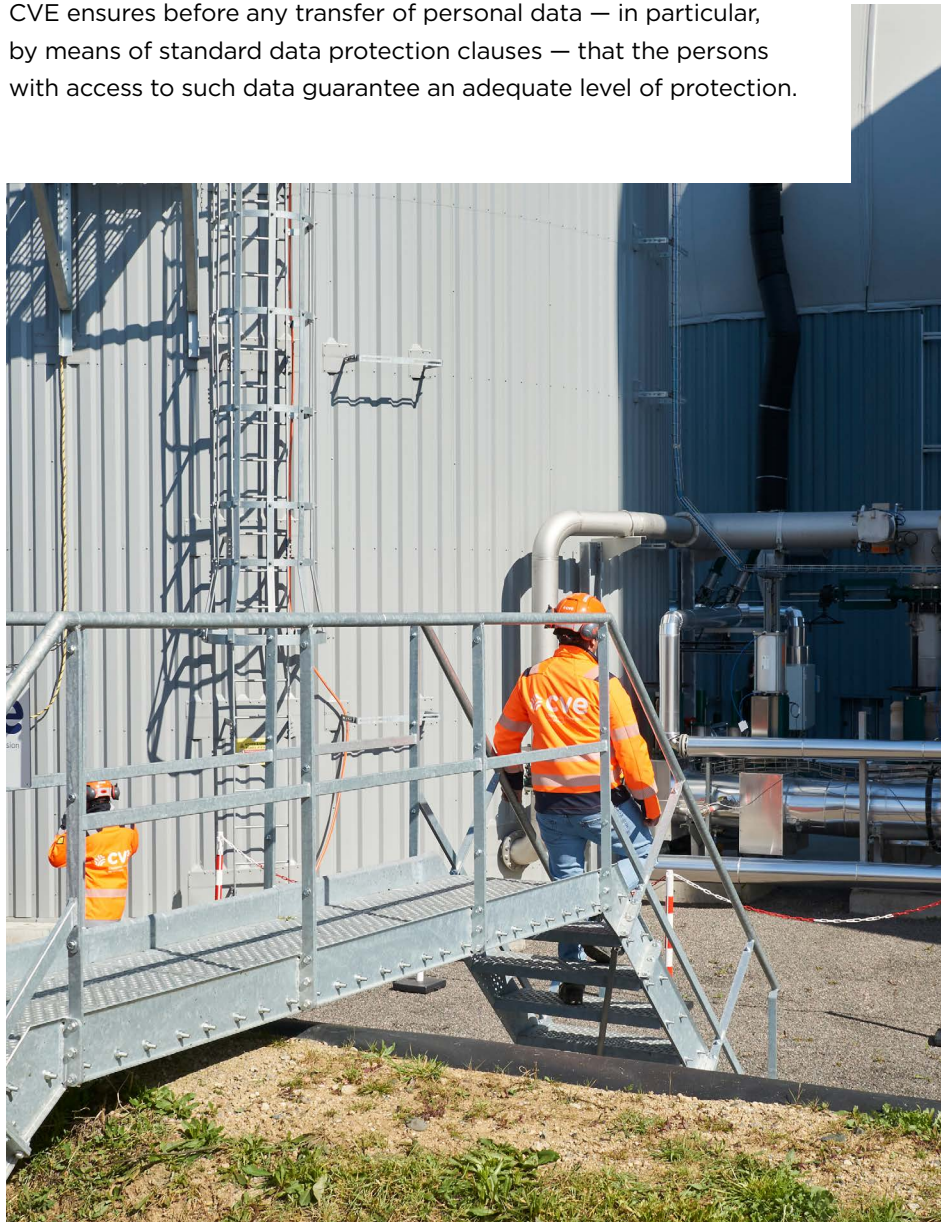
Acknowledgement of a whistleblower's complaint shall be based solely on objectively formulated data that are directly related to the scope of the whistleblower's complaint and are strictly necessary to verify the alleged facts.

4 - Recipients of the data

The data collected will be used by CVE and its affiliated companies and made accessible to third parties (such as lawyers, experts or auditors) for the purpose of their analysis and investigation as well as to CVE's technical service providers strictly for the purpose of their work.

The data collected may be made accessible outside the European Union, provided that this is strictly necessary for processing of the report received — in particular, in the context of the investigation aimed at establishing the materiality of any breaches.

CVE ensures before any transfer of personal data — in particular, by means of standard data protection clauses — that the persons with access to such data guarantee an adequate level of protection.



5 - Rights of data subjects

The author(s) of the report or all persons concerned by the report may exercise their right to access, rectify or modify data concerning themselves, by sending their request to **rgpd@cvegroup.com** and attaching any document proving their identity. They may, for legitimate reasons, oppose the processing of their data and have the right to file a complaint with the CNIL.

The subject(s) of a report may not under any circumstances obtain information concerning the identity of the author(s) of the report.

6 - Data retention period

Data relating to a report not covered by the system shall be destroyed or anonymized without delay.

Where the report is not followed by disciplinary or judicial proceedings, the data relating to the report shall be destroyed or anonymized within two months after the verification operation's closure.

When disciplinary proceedings or legal proceedings are initiated against the person(s) concerned or the author(s) of an abusive report, the data relating to the report shall be kept until the end of the disciplinary and/or legal proceedings.

At the end of these periods, the data will be archived for a period not exceeding the legal prescription periods or the applicable archiving obligations. The data subject to archiving is kept in a separate information system with restricted access. Once these periods have expired, the data will be destroyed.

APPENDIX

List of french external authorities likely to receive and process whistleblower report.

Possible alternatives to making an internal professional report.

1. Public procurement:

- Agence Française Anticorruption (AFA), for integrity violations;
- 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

2. Financial services, products and markets and prevention of money laundering and combating the financing of terrorism:

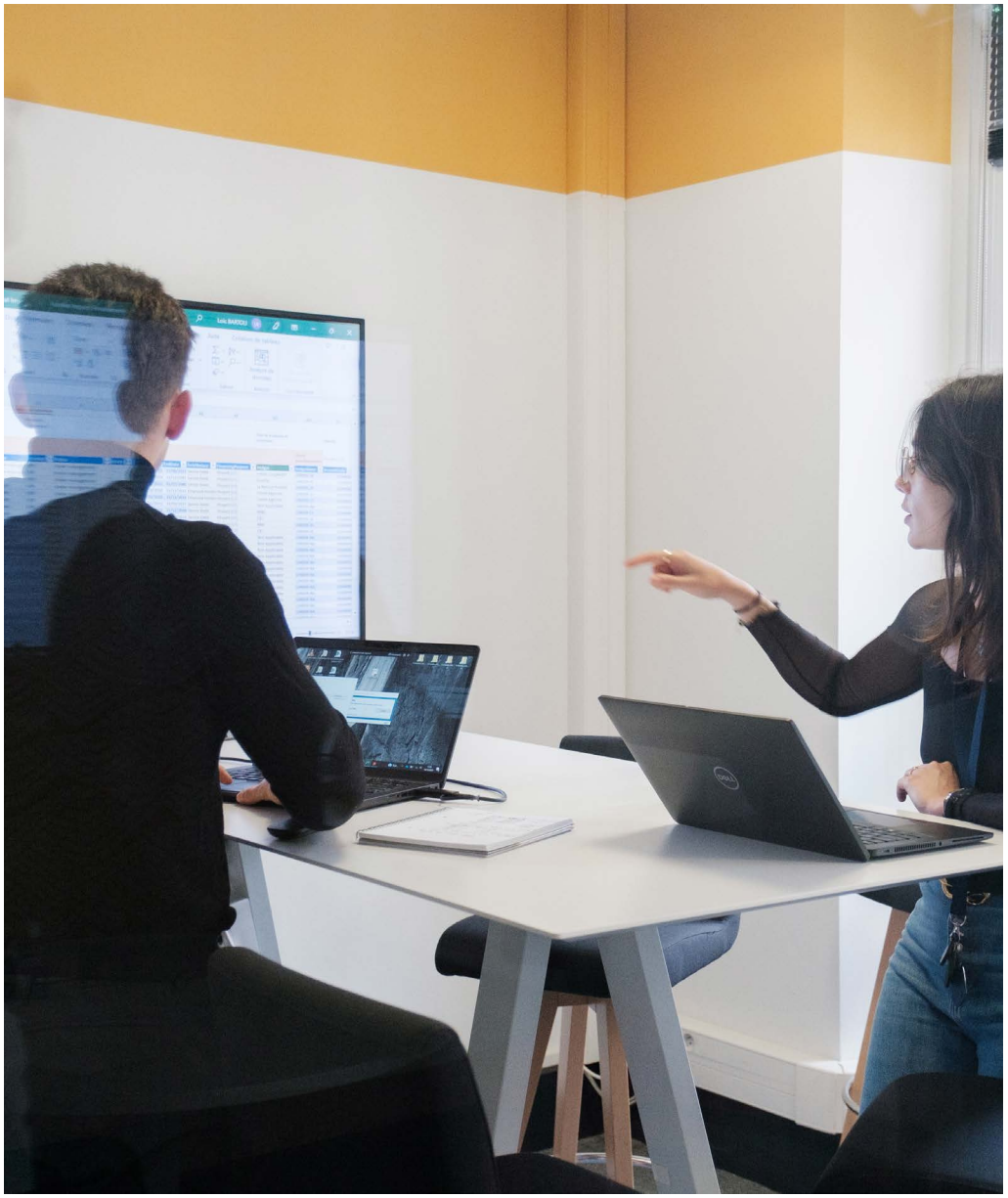
- Autorité des marchés financiers (AMF), for investment services providers and market infrastructures
- Autorité de contrôle prudentiel et de résolution (ACPR), for credit institutions and insurance companies

3. Product safety and compliance:

- Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes (DGCCRF)
- Service Central des Armes et Explosifs (SCAE)

4. Transportation safety:

- Direction générale de l'Aviation civile (DGAC), for air transport safety
- Bureau d'Enquêtes sur les Accidents de Transport Terrestre (BEA-TT), for the safety of land transport (road and rail)
- Direction générale des Affaires maritimes, de la Pêche et de l'Aquaculture (DGAMPA), for the safety of maritime transport



5. Protection of the environment:

- Inspection générale de l'Environnement et du Développement durable (IGEDD)

6. Radiation protection and nuclear safety:

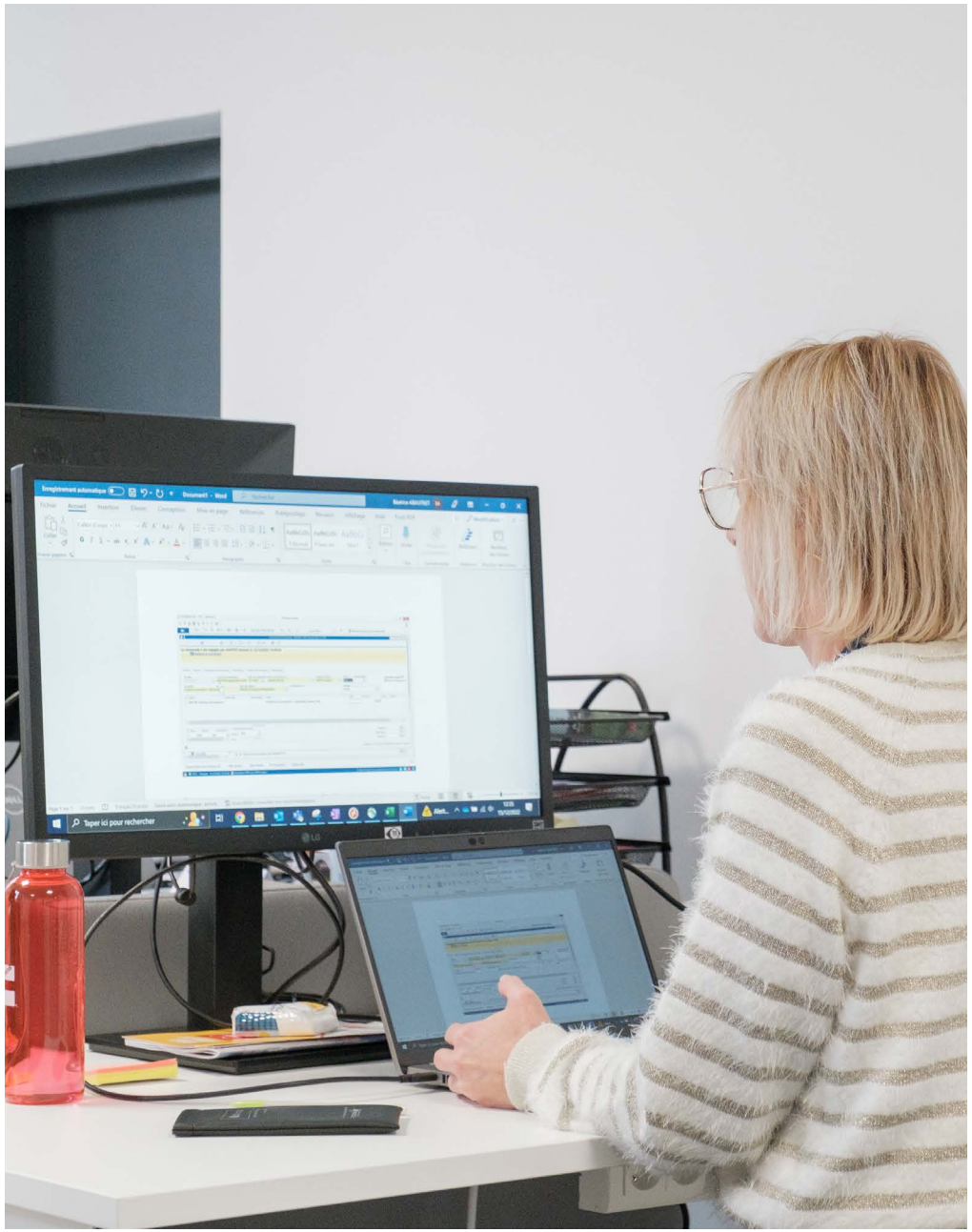
- Autorité de Sûreté Nucléaire (ASN)

7. Food Safety:

- Conseil général de l'alimentation, de l'agriculture et des espaces ruraux (CGAAER)
- Agence nationale chargée de la sécurité sanitaire de l'alimentation, de l'environnement et du travail (Anses)

8. Public Health:

- Agence nationale chargée de la sécurité sanitaire de l'alimentation, de l'environnement et du travail (Anses)
- Agence nationale de santé publique (Santé publique France, SpF)
- Haute Autorité de santé (HAS)
- Agence de la biomédecine
- Etablissement français du sang (EFS)
- Comité d'Indemnisation des Victimes des Essais Nucléaires (CIVEN)
- Inspection Générale des Affaires Sociales (IGAS)
- Institut national de la santé et de la recherche médicale (Inserm)
- Conseil national de l'ordre des médecins
- Conseil national de l'ordre des masseurs-kinésithérapeutes



- Conseil national de l'ordre des sages-femmes
- Conseil national de l'ordre des pharmaciens
- Conseil national de l'ordre des infirmiers
- Conseil national de l'ordre des chirurgiens-dentistes
- Conseil national de l'ordre des pédicures-podologues
- Conseil national de l'ordre des vétérinaires

9. Consumer Protection:

- Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes (DGCCRF)

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

- Commission Nationale de l'Informatique et des Libertés (CNIL)
- Agence nationale de la sécurité des systèmes d'information (ANSSI)

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

- Agence Française Anticorruption (AFA), for integrity violations
- Direction générale des Finances Publiques (DGFiP), for value added tax fraud
- Direction générale des douanes et droits indirects (DGDDI), for fraudulent customs duties, anti-dumping duties and the like

12. Violations related to the internal market:

- 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 and State aid
- Direction générale des Finances Publiques (DGFiP), for corporate tax fraud

13. Activities conducted by the Ministry of Defense:

- Contrôle général des Armées (CGA)
- Collège des inspecteurs généraux des armées

14. Public Statistics:

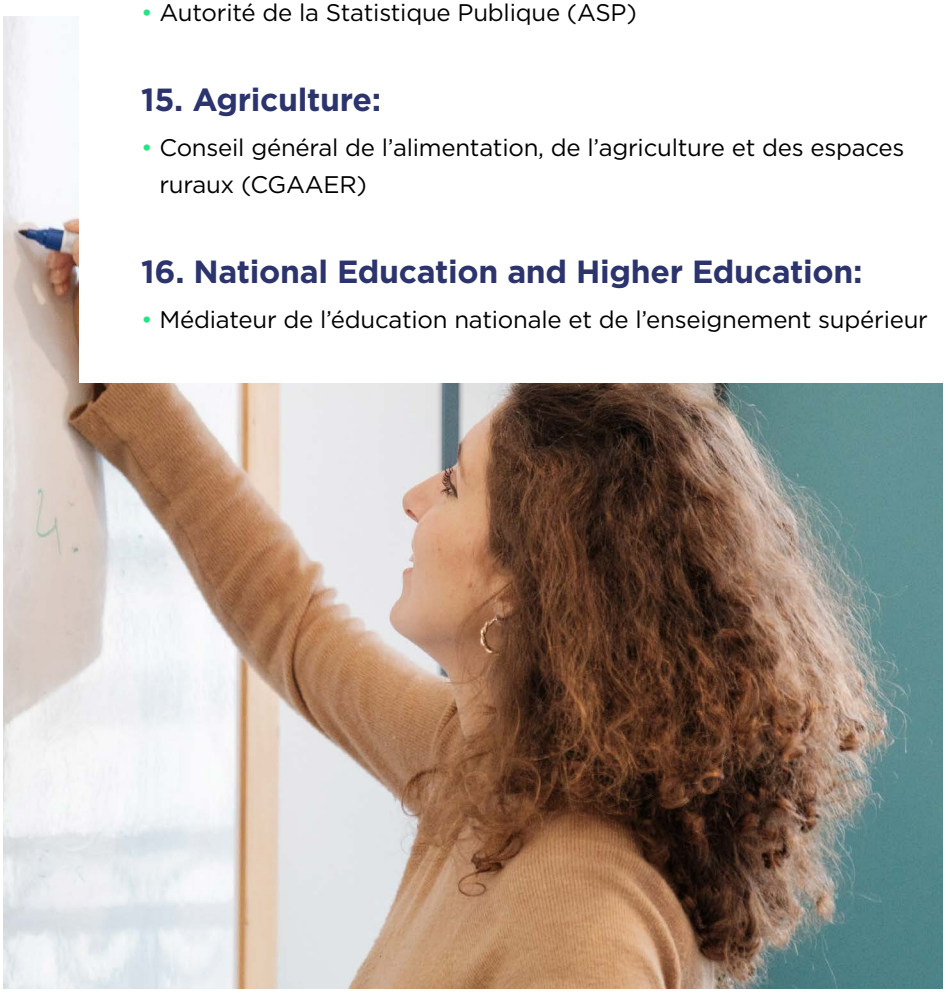
- Autorité de la Statistique Publique (ASP)

15. Agriculture:

- Conseil général de l'alimentation, de l'agriculture et des espaces ruraux (CGAAER)

16. National Education and Higher Education:

- Médiateur de l'éducation nationale et de l'enseignement supérieur



17. Individual and collective labor relations, working conditions:

- Direction générale du travail (DGT)

18. Employment and professional training:

- Délégation générale à l'emploi et à la formation professionnelle (DGEFP)

19. Culture:

- Conseil national de l'ordre des architectes, for the practice of the profession of architect
- Conseil des ventes, for public auctions

20. Rights and freedoms in the context of relations with State administrations, local authorities, public establishments and organizations with a public service mission:

- Défenseur des droits

21. Best interests and rights of the child:

- Défenseur des droits

22. Discrimination:

- Défenseur des droits

23. Ethics of persons performing security activities:

- Défenseur des droits