

Alerte (☎) Professionnelle

Confidentiality policy

Introduction

CCF Holding and all its subsidiaries - Groupe CCF (hereinafter referred to as "we", "us" or "our") are committed to respecting your privacy and protecting your personal data.

The purpose of this Personal Data Protection Policy (hereinafter the "Policy") is to provide you with a clear and transparent overview of the personal data protection arrangements put in place for the management of Career Alerts.

Personal data" refers to any information that can directly or indirectly identify you (e.g. surname, first name, photograph, IP address).

Groupe CCF undertakes to comply with the laws and regulations applicable to the protection of personal data, and in particular Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter "RGPD") and Law No. 78/17 of 6 January 1978, as amended, known as the "Data Protection Act".

Table of contents

1.	Who is the Data Controller?	1
2.	What personal data do we collect and process under the scheme?	2
3.	With whom are we likely to share your personal data?	2
4.	For what purposes are your data processed?	3
5.	How do we protect your personal data?	3
6.	How long do we keep your personal data?	3
7.	Is your data transferred outside the European Union (EU)?	3
8.	What rights do you have?	3
9.	How can I contact the Data Protection Officer?	4
10.	Updating the Policy	4

1. Who is the Data Controller?

The data controller is the entity that determines why and how applicants' data is processed.

Groupe CCF is responsible for processing the personal data it collects as part of setting up and managing the professional alerts system.

2. What personal data do we collect and process under the scheme?

The use of the professional alerts system requires the processing of various categories of information, including personal data.

- **When you report information about an alert :**

We collect and process data about you when you submit your alert on the platform, and also as we investigate the events covered by the alert.

This includes the following information:

- Full name
- Country
- Function
- Department
- Business address
- Personal address
- Contact telephone number
- Information relating to the alert, such as the facts reported, the people involved and the associated documents.

As the collection of certain data is optional, data that must be provided is marked with an asterisk in the reporting platform.

- **When you are reported as being responsible for the behaviour that is the subject of the alert:** we collect information about you when you are reported as being responsible for the facts relating to the alerts. This collection is carried out mainly to comply with our regulatory obligations.

Depending on the facts reported and the subject of the alert, sensitive data about you may be processed. Sensitive data includes information relating to your health, ethnic origin, religious or political beliefs (article 9 of the RGPD), or information relating to criminal convictions and offences (article 10 of the RGPD).

This is particularly the case when the declaration concerns a case of discrimination, infringement of human rights or fundamental freedoms.

3. With whom are we likely to share your personal data?

The information collected is strictly confidential and will never be disclosed without the user's consent, except where required by law.

Where justified by the alert raised, your data will be sent to:

- **Group entities**

We may transfer your data to other entities to ensure the proper handling of the alert.

- **Administrative and judicial authorities:**

If the alert gives rise to possible legal or criminal proceedings, we will be legally obliged to transfer your data to the competent authorities for processing.

4. For what purposes are your data processed?

The information collected from users of the whistleblowing platform is used for the following purposes:

- Handle alerts reported via the platform;
- To enable communication between our company and the user, if necessary;
- Meeting our legal obligations;
- Protect the information collected.

5. How do we protect your personal data?

We deploy technical and organizational security measures to protect information collected from users against loss, destruction, disclosure or unauthorized access.

We do not pass on the information collected to third parties, unless required by law.

6. How long do we keep your personal data?

The length of time your personal data is kept depends on the action taken in response to the alert.

Qualification of the alert		Shelf life
Alert not covered by the scheme		Immediate deletion of data
Alert within the scope of the system	No follow-up	Deletion of data within two months of the end of the investigation
	Initiation of proceedings (contentious or disciplinary)	Retention of data until the end of the procedure and until all appeals have been exhausted or the statute of limitations on appeals against the decision has expired.

7. Is your data transferred outside the European Union (EU)?

No data is transferred outside the European Union as part of the scheme. All data is processed and stored in France.

8. What rights do you have?

You have control over your personal data. As a data subject, you can contact us to exercise your rights.

You have the following rights regarding your personal data:

- **Right to information:** you have the right to ask us questions about how we process your personal data.

- **Right of access:** you have the right to ask us to confirm that your personal data is being processed by our services. Where appropriate, at your request, we will send you a copy of your personal data that is being processed.
- **Right to rectification:** you have the right to have inaccurate personal data processed by us rectified or completed.
- **Right to erasure:** you have the right to obtain the erasure of your personal data as soon as possible when it is no longer required for the purposes for which it was collected.
- **Right to restriction:** you have the right to obtain restriction, i.e. a freeze on the processing of your personal data, in particular where this is necessary for the establishment, exercise or defence of your legal rights.
- **Right to object:** you have the right to object at any time, for reasons relating to your particular situation, to the processing of your personal data. This right may only be overridden by legitimate and compelling reasons of the employer or the establishment, exercise or defense of legal claims.
- **Right to portability:** you have the right to receive the personal data you have provided in a structured, commonly used and machine-readable format.
- **Right to object to automated decisions:** you have the right to object to decisions based solely on automated processing that may include profiling or any other decision that could affect you legally or significantly.
- **Right to give instructions on what to do with your data after your death:** you can give instructions on the storage, deletion, and communication of your personal data after your death.

- **How to exercise your rights:**

If you wish to exercise a right, or if you have a disagreement or complaint about the processing of your personal data, you can send a request to the Data Protection Officer by the following means:

- Postal mail: For the attention of CCF Holding - Data Protection Officer - Tour Europlaza 20 Avenue André prothin 92063 Paris La Défense Cedex
- E-mail: DPO-Groupe@MyMoneyGroup.com

In case of doubt, we may ask you for additional information to verify your identity.

- **How do I lodge a complaint with the CNIL?**

If, after contacting us, you feel that your rights have not been respected, you can send a complaint to the CNIL at the following address: Commission nationale de l'informatique et des libertés - 3 Place de Fontenoy - TSA 80715 - 75334 Paris CEDEX 07.

9. How can I contact the Data Protection Officer?

If you would like to know more about the provisions of this policy or contact our Data Protection Officer, you can write to us at the following addresses:

- Postal mail: For the attention of CCF Holding - Data Protection Officer - 103 Rue de Grenelle, 75007 Paris
- E-mail: DPO-Groupe@MyMoneyGroup.com

10. Policy update

We may amend this document in order to update it, to take account of legal and regulatory developments or to provide you with new information about the processing of your data that we carry out.

The last update dates from 15 January 2024.