Speak Up Privacy Policy

Any personal data collected, stored, used or disclosed under this Policy will be managed in accordance with Speak Up Privacy Policy.

1. Purpose and legal basis

The Speak Up portal provides a space to report and manage alerts related to criminal offenses and infringements to Expleo's Code of Conduct and related applicable legislations. Those include, but are not limited to:

- The French «Sapin II» Law, including the provisions regarding the protection of whistleblowers (art. 6-16) and those relating to measures to fight corruption (art. 17).
- The French Law on the duty of vigilance.
- The EU Directive on the protection of whistleblowers: it aims to establish common minimum standards of protection across the EU for whistleblowers who signal violations of any applicable laws and regulations to their employer. This requires the establishment of a whistleblower system as well as a whistleblower procedure with a secure reporting channel. The EU Directive also requires that any individual who notifies their employer of wrongdoing must be afforded protection from retaliation.
- General legislative measures for the protection of individuals (including provisions on sexual and moral harassment, as well as all forms of discrimination).
- Where applicable, local legislations related to similar topics.

Personal data is collected and processed for the purposes of assessing the admissibility of the report, of checking facts and taking appropriate measures, if necessary. It also enables Expleo to comply with its legal obligations and to protect its legitimate interests (respect of the law and of the Code of Conduct).

Consequently, the data processing is based on

- The legitimate interest of Expleo, when the report falls outside of the scope of the legislations mentioned above ;
- Compliance with a legal obligation in relation with the management of professional alert system and other equivalent legislations related to the management of alerts related to sexual and moral harassment or any other form of discrimination.

2. Processing of personal data

When making a report, a Reporter may communicate to Expleo personal data relating to them and also relating to the person(s) implicated by the report and/or the person(s) who could provide information necessary for the handling of the report.

Moreover, Expleo may collect and handle personal data concerning other person(s) during the handling of the report.

- During the emission of the report:

When completing a report, only the Reporter is able to determine the nature and volume of information, particularly of a personal nature, communicated in the report. Therefore, the Reporter is reminded that the information communicated as part of the Speak Up Policy must remain factual and present a direct link with the subject of the alert.

Based on the willingness of the Reporter, the types of personal data that can be collected and processed may include:

- Identity, function and contact detail of the Reporter
- Identity, function and contact detail of the person(s) implicated by the report
- As well as any other information voluntarily communicated by the Reporter or resulting from the handling of the report.

- When Expleo manages the report:

Once a report has been submitted, it will be managed by Expleo. This phase allows the organization to conduct an investigation into the facts reported. During this period, the system can be used to document the steps taken by the organization in this regard (analysis legal and technical facts, collection of evidence, exchanges with various stakeholders, hearing of witnesses, performance of expert reports, etc.).

Consequently, when handling a report, Expleo may also collect personal data concerning person(s) who may provide information necessary for the handling of the report (these persons may have been identified by the Reporter or not).

Depending on the circumstances and the information provided in the report, Expleo might process the following personal data:

- identity, functions and contact details of the Reporter of the alert;
- identity, functions and contact details of the persons subject to the alert;
- identity, functions and contact details of the persons involved in the collection or in the alert processing;
- reported facts and elements collected as part of the verification of the facts reported;
- reports of verification operations and follow-up given to the alert.

It is understood that depending on the information provided in the report, it will include any person mentioned. This may include:

- The staff of the organization concerned, regardless of the legal status of the collaboration (employees, agents, temporary workers, trainees, employees seconded by a third-party entity, volunteers, etc.) ;
- Employees, customers and external suppliers of the organization, when they are people natural persons having a direct contractual link with the organization (consultants, agents, advisers, subcontractors natural persons with self-employed status, etc.);
- The workforce (employees, partners, managers, etc.) of legal persons who maintain a link contract with the organization concerned.

3. Data controllers and data transfers

The person responsible for data processing within the meaning of the General Data Protection Regulation (GDPR) and other data protection provisions is:

- EXPLEO GROUP S.A.S., Registered Office: 3 Avenue des Prés, 78180 Montigny-le-Bretonneux, France A French company governed by French law, Simplified joint stock company with capital of 242,397,967.00 euros – Registered on the Trade and Companies Register under number 831 178 785 RCS Versailles
- Phone: +33 130122500
- The designated data protection officer can be reached at: dpo@expleogroup.com

However, Data Subjects are informed that considering the nature of the data processing, when handling a report, personal data may be collected or processed by, or transferred to other entities of the Expleo group, for example, the entity where the relevant Employee is employed or located. In this case, these entities also act as data controller.

Your personal data will be hosted in a datacentre in Europe. But this data processing might involve entities that are located outside of the European Union. Although the group has separate legal entities (for example, national subsidiaries) in many countries, our internal processes and infrastructure are international in scope and nature and are generally transnational. As a result, we inform you that we may share your personal data with other Expleo entities on a need-to-know basis and transfer it to the countries where the report shall be instructed, including in countries outside the European Union (EU). These data transfers will benefit from the same level of protection as data that is processed within the EU and as such, if applicable, they may be subject to intra-group agreements for the transfer of personal data.

4. Retention

Subject to document retention requirements of local legislation, data relating to an alert considered by the controller as not falling within in the field of the device, are destroyed without delay or anonymized.

When no follow-up is given to an alert falling within the scope of the system, the data relating to this alert are destroyed or anonymized by the organization in charge of managing the alerts, in a period of two months from the end of the verification operations. For present purposes framework, the expression “follow-ups” refers to any decision taken by the organization to derive consequences of the alert. This may involve the adoption or modification of internal rules (regulations internal, ethical charter, etc.) of the organization, a reorganization of operations or services of the company, the imposition of a sanction or the implementation of a legal action.

When disciplinary or contentious proceedings are initiated against a person placed under cause or the author of an abusive alert, the data relating to the alert may be kept by the organization responsible for managing alerts until the end of the procedure or prescription of appeal against the decision. With the exception of cases where no follow-up is given to the alert, the data controller may keep the data collected in the form of intermediate archives for the purpose of ensuring the protection of the Reporter of the alert or to allow the observation of continuous infringements.

Subject to local legislations, the data may be kept longer, in intermediate archiving, if the person in charge of the processing has a legal obligation (for example, to meet accounting, social or taxes).

5. Data recipient

Persons who may access personal data communicated or collected are the Group Compliance Officer, persons appointed by them to handle a report and more generally all persons to which they may have recourse in order to receive and/or handle a report or to take appropriate measures, in compliance with this Speak Up Policy.

This may include individuals within Expleo or its Subsidiaries. The referent or service provider of service possibly designated to manage all or part of this process undertakes in particular, by contractual way, not to use the data for purposes other than the management of alerts, to ensure their confidentiality, to respect the limited retention period of the data and to proceed with the destruction or the return of all manual or computerized personal data media to the term of his service.

In this regard, if a report was made through the secure Speak Up portal, Expleo external service provider, Gan Integrity, is also considered as data recipient.

All these persons are bound by a strict confidentiality obligation.

Depending on the nature of the information present in the report, Expleo may also be required – by law, legal proceedings, litigation and/or requests from public and government authorities in or outside your country of residence – to disclose your personal data to the authorities. Expleo may also disclose your personal data if we believe it is necessary or appropriate for reasons of national security, law enforcement or other matters of public interest.

6. Data Subjects Rights

Depending on your location and subject to applicable law, you may have the following rights described here with regard to the Personal Data Expleo process in the context of the Speak Up Policy:

- Subject to limitation related to the nature of the report, the right to request confirmation of whether Expleo processes Personal Data relating to you, and if so, to request a copy of that Personal Data;
- Subject to limitation related to the nature of the report, the right to request to rectifies or updates your Personal Data that is inaccurate, incomplete or outdated;
- Subject to limitation related to the nature of the report, the right to request that Expleo erase your Personal Data in certain circumstances provided by law;
- Subject to limitation related to the nature of the report, the right to request that Expleo restrict the use of your Personal Data in certain circumstances;
- Where the processing of your Personal Data is based on your previously given consent, you have the right to withdraw your consent at any time, unless the nature and circumstances related to the report and the applicable legislation restrict such right.

Your rights might be exerted by sending an email to dpo@expleogroup.com

However, it is reminder that considering the specific nature of the data processing related to the Speak Up Policy, these rights cannot be used to prevent Expleo from fulfilling its legal obligation to handle report and protect Reporters. For legal reasons, Expleo might be subject to compelling legitimate grounds or applicable legislation that would be obstacle to the exercise of your rights.

Without prejudice to any other administrative or judicial remedy, every Data Subject have the right to lodge a complaint with the supervisory authority of its country.

To obtain more information on how personal data is collected and processed by Expleo, data subjects can send a request to: dpo@expleogroup.com.