ALLEN & OVERY

Extended and enhanced legal protection for whistleblowers and increased obligations for employers in Luxembourg

2 May 2023

Adoption today (02 May 2023) of bill no. 7945 aiming to transpose the European directive on persons who report breaches by a company (the "whistleblowers"), via internal or external channels (to the authorities), or by public disclosure (via the press, the media). Whistleblowers will benefit from a protection regime aiming to guarantee their anonymity and employment.

Below, an overview of the new law (hereinafter the **Law**) whose entry into force is planned 4 days after the publication of the text in the *Mémorial*, with a publication expected in the next few weeks.

For companies with 250 employees or more, the obligation to set up internal reporting channels will be immediate, while companies with between 50 and 249 employees will have until 17 December 2023 to comply with this obligation.

A reporting office, specially created, as well as several authorities declared competent in the matter (including the Financial Regulator - the CSSF, the Labour Inspectorate - the ITM, and the Data Protection Authority - the CNPD) will be in charge of monitoring compliance with the new provisions and mainly the setting up of internal reporting channels, with a possibility to issue significant administrative fines.

Triggering of the protection: launching the alert *via* the reporting channels

In order to ensure the protection of whistleblowers, the setting up of internal and external reporting channels, as well as in some cases, the possibility of public disclosure, are regulated. We will present exclusively the obligations incumbent on employers.

The obligation to set up internal reporting channels

Any company with at least 50 employees must establish channels and procedures for internal reporting and its follow-up.

There are exceptions to this minimum threshold. In particular, alternative investment fund managers (AIFM) are subject to this obligation regardless of the number of employees they occupy.

The Law lists the elements that any internal reporting and follow-up procedure must include, in particular:

- secure reporting channels protecting the identity of the whistleblower and of any third party mentioned;
- an acknowledgement of receipt sent to the whistleblower within seven days;
- a reasonable time limit, not exceeding three months, for providing feedback on the measures envisaged or taken as part of the follow-up.

These channels must allow reports to be made in writing or orally, in French, German or Luxembourgish, or in any other language accepted by the company.

The obligation of a diligent follow-up implies assessing the accuracy of the allegations made by the whistleblower, in particular by conducting an internal investigation.

Any processing of personal data carried out in this context must comply with the General Data Protection Regulation (GDPR) and in particular with the principle of data minimisation (i.e. only the data relevant for the reporting may be processed).

Reporting channels may be operated internally by a person or department designated for that purpose or provided externally by a third party. A sharing of resources is possible for companies employing between 50 and 249 employees (for instance by organizing a common service).

The establishment of the channels and procedures for internal reporting and their follow-up will require the involvement of the staff delegation, if there is one.

In order to prioritize internal reporting and thus minimise the risk of financial and reputational impact, it is recommended to ensure the simplicity of use, as well as the attractiveness of the internal reporting channels. In this regard, the implementation of a digital whistleblowing system, compliant with the GDPR, has the advantage of guaranteeing the security and anonymity of whistleblowers.

Extended and reinforced protection regime[1]

Beneficiaries of the protection beyond the employees of the company

The protection is very broad and benefits not only the employees, shareholders, members of the governing, managing or supervisory body of any company concerned by the alert, but also the volunteers, interns, subcontractors, independent contractors, facilitators, and even third parties who are in contact with the whistleblowers (colleagues, staff representatives, relatives).

The information that can give rise to reporting can have been obtained before the start of the employment relationship (for example, during the recruitment phase), during the employment relationship or even when it has ended.

The reporting of a violation of any provision of national or European law

Whistleblowers who, in the course of their professional activities, report acts or omissions violating any provision whatsoever of national or European law will benefit from the protection.

The prohibition of retaliation and the immunity from liability

As long as they acted in good faith, the whistleblowers, as well as the facilitators or third parties, are **protected against any form of retaliation** for reporting. Any disciplinary measure taken because of a report is therefore null and void.

Besides a court action for annulment of the disciplinary measure, whistleblowers can bring a judicial action for compensation of the prejudice suffered. Whistleblowers benefit from a presumption of causal link. Indeed, if the whistleblowers prove that they made a report through the established channels and that they suffered a prejudice, this prejudice is presumed to result from the retaliation for the report. In this case, it is up to the employer to rebut this presumption by establishing separate reasons (which must be the precise, real and serious) that justify the measure.

Whistleblowers will not be held liable for the means used to obtain the information disclosed if they have reasonable grounds to believe that their report is necessary to reveal a violation (e.g.: if the whistleblower copies documents that he/she takes out of the company in breach of contractual clauses).

Sanctions regime

A fine of up to EUR 25,000 is provided for any person who exercises retaliation.

[1] In the area of financial services, detailed rules on the protection of whistleblowers already exist. These special sectoral laws will, in principle, not be affected by the general provisions of this Law.

Moreover, an administrative fine of up to EUR 250,000 can be imposed on natural and legal persons who, among other things:

- obstruct a report; or
- do not establish the channels and procedures for internal reporting and its follow-up.

It should also be noted that anyone who knowingly reports false information will be liable to a prison sentence and/or a fine of up to EUR 50,000.

Allen & Overy Luxembourg will be happy to assist you in setting up the channels and procedures for internal reporting and its follow-up.

ALLEN & OVERY

Protection légale étendue et renforcée pour les lanceurs d'alerte et obligations accrues pour les employeurs au Luxembourg

2 mai 2023

Adoption aujourd'hui (02 mai 2023) du projet de loi n°7945 visant à transposer la directive européenne sur les personnes qui signalent des violations par une entreprise (les « lanceurs d'alerte »), via des canaux internes (par exemple à leur hiérarchie) ou externes (aux autorités), ou par divulgation publique (via la presse, les médias). Les lanceurs d'alerte bénéficieront d'un régime de protection visant à garantir leur anonymat et leur emploi.

Ci-dessous, un aperçu de la nouvelle loi (ci-après la **Loi**) dont l'entrée en vigueur est prévue 4 jours après la publication du texte au Mémorial, publication attendue dans les toutes prochaines semaines.

Pour les entreprises comptant 250 salariés et plus, l'obligation de mise en place de canaux internes de signalement sera immédiate, tandis que les entreprises employant entre 50 et 249 salariés auront un délai supplémentaire jusqu'au 17 décembre 2023 pour se conformer à cette obligation.

Un office des signalements, spécialement créé, ainsi que plusieurs autorités déclarées compétentes en la matière (dont la Commission de surveillance du secteur financier – la CSSF, l'Inspection du travail et des mines – l'ITM, et la Commission nationale pour la protection des données – la CNPD) seront chargés de surveiller le respect des nouvelles dispositions et principalement la mise en place de canaux de signalement interne au sein des entreprises, sous peine d'amende administrative importante.

Déclenchement de la protection : le lancement de l'alerte *via* les canaux de signalement

Afin d'assurer la protection des lanceurs d'alerte, la mise en place de canaux de signalement interne et externe, ainsi que dans certains cas, la possibilité d'une divulgation publique, sont encadrées. Nous présenterons exclusivement les obligations à charge des employeurs.

L'obligation de mise en place de canaux de signalement interne

Toute entreprise de 50 salariés au moins doit établir des canaux et des procédures pour le signalement interne et son suivi.

Il existe des exceptions par rapport à ce seuil minimal. Notamment, les gestionnaires de fonds d'investissement alternatifs (GFIA ou AIFM) sont soumis à cette obligation quel que soit le nombre de salariés qu'ils occupent.

La Loi énumère les éléments que toute procédure de signalement interne et de suivi doit inclure, en particulier :

- des canaux de signalement sécurisés protégeant l'identité du lanceur d'alerte et de tout tiers mentionné;
- un accusé de réception adressé au lanceur d'alerte dans un délai de sept jours ;
- un délai raisonnable, n'excédant pas trois mois, pour fournir un retour d'informations sur les mesures envisagées ou prises au titre du suivi.

Ces canaux doivent permettre d'effectuer des signalements par écrit ou oralement, en français, allemand ou luxembourgeois, ou dans toute autre langue admise par l'entreprise.

L'obligation d'un suivi diligent implique d'évaluer l'exactitude des allégations faites par le lanceur d'alerte, notamment en réalisant une enquête interne.

Tout traitement de données à caractère personnel effectué dans ce contexte devra être conforme au Règlement Général sur la Protection des Données (RGPD) et notamment au principe de minimisation des données (c.-à-d. uniquement les données pertinentes pour le signalement pourront être traitées).

Les canaux de signalement peuvent être confiés à une personne ou un service en interne ou à un prestataire externe. Un partage des ressources est possible pour les entreprises occupant entre 50 et 249 salariés (par exemple en organisant un service commun).

L'établissement des canaux et des procédures pour le signalement interne et leur suivi nécessitera l'implication de la délégation du personnel, s'il y en a une.

Afin de privilégier le signalement interne et ainsi minimiser le risque d'un impact financier et réputationnel, il est recommandé d'assurer la simplicité d'utilisation, ainsi que l'attractivité des canaux

de signalement interne. A cet égard, la mise en place d'un système de dénonciation digital, conforme au RGPD, présente l'avantage de garantir la sécurité et l'anonymat des lanceurs d'alerte.

Régime de protection étendu et renforcé[2]

Des bénéficiaires de la protection au-delà des seuls salariés de l'entreprise

La protection est très large et profite non seulement aux salariés, actionnaires, membres de l'organe d'administration, de direction ou de surveillance de toute entreprise concernée par l'alerte, mais également aux bénévoles, stagiaires, sous-traitants, indépendants, facilitateurs, et jusqu'aux tiers qui sont en lien avec le lanceur d'alerte (collègues, délégués du personnel, proches).

Les informations pouvant donner lieu à signalement peuvent avoir été obtenues avant le début de la relation de travail (par exemple, lors de la phase de recrutement), pendant la relation de travail ou encore lorsque celle-ci a pris fin.

Le signalement d'une violation quelconque du droit national ou européen

Bénéficieront de la protection les lanceurs d'alerte qui, dans le cadre de leurs activités professionnelles, signalent des actes ou omissions violant une disposition quelconque du droit national ou européen.

L'interdiction des représailles et l'immunité de responsabilité

Pour autant qu'ils aient été de bonne foi, les lanceurs d'alerte, ainsi que les facilitateurs ou les tiers, sont protégés contre toutes formes de représailles en raison du signalement. **Toute mesure disciplinaire prononcée en raison d'un signalement est de ce fait nulle.**

Outre une action en nullité, le lanceur d'alerte peut exercer une **action judiciaire en réparation** du dommage subi. Le lanceur d'alerte bénéficie d'une présomption relative au lien de causalité. En effet, s'il établit qu'il a effectué un signalement via les canaux établis et qu'il a subi un préjudice, ce préjudice est présumé résulter des représailles du signalement. Dans ce cas, il incombe à l'employeur de renverser cette présomption en établissant les motifs distincts (qui doivent être précis, réels et sérieux) qui fondent la mesure.

Le lanceur d'alerte ne sera pas tenu responsable des moyens utilisés pour obtenir les informations dévoilées s'il a des motifs raisonnables de croire que son signalement est nécessaire pour révéler une violation (ex.: si le lanceur d'alerte copie des documents qu'il emporte hors de l'entreprise en violation de clauses contractuelles).

[2] Dans le domaine des services financiers des règles détaillées sur la protection des lanceurs d'alerte existent déjà. Ces lois spéciales sectorielles ne seront en principe pas affectées par les dispositions générales.

Régime des sanctions

Une amende jusqu'à EUR 25.000 est prévue à l'encontre de toute personne qui exercerait des représailles.

Par ailleurs, une amende administrative jusqu'à EUR 250.000 peut être prononcée à l'encontre des personnes physiques et morales qui, notamment :

- entravent un signalement ; ou
- n'établissent pas les canaux et les procédures pour le signalement interne et son suivi.

A noter également que celui qui a sciemment signalé de fausses informations sera passible d'une peine d'emprisonnement et/ou d'une amende jusqu'à EUR 50.000.

Allen & Overy Luxembourg sera heureux de vous accompagner dans la mise en œuvre des canaux et des procédures pour les signalements internes et leur suivi.

For further information on the topic, please reach out to your usual A&O contact, or any of the below relevant contacts.

Gilles Dall'Agnol

Partner
Tel +352 44 44 5 5104
gilles.dallagnol@allenovery.com

André Marc

Of Counsel
Tel +352 44 44 5 5509
andre.marc@allenovery.com

Christophe Ernzen

Counsel
Tel +352 44 44 5 5112
christophe.ernzen@allenovery.com

Maurice Macchi

Counsel
Tel +352 44 44 5 5231
maurice.macchi@allenovery.com

Gabrielle Eynard

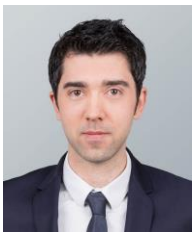
PSL-Senior Associate
Tel: +352 44 44 5 5115
gabrielle.eynard@allenovery.com

Nathaël Malanda

Senior Associate
Tel +352 44 44 5 5206
nathael.malanda@allenovery.com

Laurie Lougsami

Senior Associate
Tel +352 44 44 5 5299
laurie.lougsami@allenovery.com



Julian Kisslinger

Associate
Tel +352 44 44 5 5316
julian.kisslinger@allenovery.com

Clara Duc

Associate
Tel +352 44 44 5 5180
clara.duc@allenovery.com

Eric Weber

Associate
Tel +352 44 44 5 5462
eric.weber@allenovery.com

Laure Varichon

Junior Associate
Tel +352 44 44 5 5510
laure.varichon@allenovery.com