EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE AND CONSUMERS

Directorate C : Fundamental Rights and Rule of Law
Unit C2 : Fundamental Rights Policy
Acting Head of Unit

Brussels, 02.06.2021
JUST/C2/MM/rp/ (2021)3939215

Confederation of Danish Industry
[redacted]
Svenskt Näringsliv
[redacted]
BDA Die Arbeitgeber
[redacted]
BDI
[redacted]
IBEC for Irish Business
[redacted]
Confederation of Industry of the Czech Republic
[redacted]
Business Europe
[redacted]

Dear Sirs, Madams,

Subject: **Your joint letter regarding the EU Whistleblower Directive (our ref. Ares(2021) 3355262)**

I refer to your joint letter of 19 May and to the letter addressed by some Danish companies to the Danish Parliament, which you sent to us on 27 May, seeking our views on the concerns expressed therein.

In your joint letter you ask if the Commission could reconsider its interpretation of Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law ("the Whistleblower Directive"), to the extent that it prevents group solutions for entities with 250+ workers, namely that one of the legal entities in the group, e.g. one which runs group function, may operate a uniform whistleblowing scheme with reporting channels on behalf of group companies/legal entities.

The letter addressed by some Danish companies to the Danish Parliament pleads for the same outcome.

Let me start by recalling that the objective of the Directive is to enhance the enforcement of Union law and policies by providing a high level of protection to whistleblowers: the more whistleblowers feel safe to speak up, the higher the number of whistleblowers' reports, which will feed national and Union enforcement systems.

Article 8(3), which provides that "*Paragraph 1 [the obligation to establish channels and procedures for internal reporting] shall apply to legal entities in the private sector with 50 or more workers*", does not make any exemption for distinct legal entities belonging to the same corporate group. This entails that reporting channels *cannot* be established in a centralised manner only at group level; all medium-sized and large companies belonging to a group remain obliged to have each their own channels.

This is justified by the need to ensure the reporting channels' efficiency, including by ensuring their proximity to the whistleblower. To facilitate reporting i) channels must be easily accessible, ii) comprehensive information on their use and on the procedures for reporting externally to competent authorities must be provided on the website and/or premises of the legal entity where the whistleblower works,[1] iii) an impartial person/department in the legal entity where the whistleblower works must be designated to follow up on the report, give feedback to the whistleblower and maintain communication with him/her; iv) depending on how the national transposition law transposes the provision in Article 9(2), whistleblowers may have the right to request a physical meeting in the company with which they have a work-related relation.

Moreover, the Directive encourages legal entities to open reporting channels also to external persons having a work-related relation with the company in question (self-employed, contractors, sub-contractors etc. – see Article 8(2), 2nd sentence). For these persons, the proximity of internal channels and procedures would be particularly important because they are only familiar with the company they work with/for.

Additional reasons come into play where the companies of a same group are located in different Member States, as relevant rules may differ depending on the transposition laws of the Member States concerned. To mention a few examples:

- first, each Member State may decide to transpose the material scope of the Directive exactly as defined in the Directive, or to extend the protective regime of the Directive also to reports of breaches of national law in the policy areas covered by the Directive or even beyond those policy areas. As a result, the Directive would apply or not to the report of a breach falling outside its material scope depending on the transposition law of the respective Member State (e.g. a breach may be covered

[1] See Recital 59 *in fine*: "It is essential that such information be clear and easily accessible, including, to any extent possible, also to persons other than workers, who come in contact with the entity through their work-related activities, such as service-providers, distributors, suppliers and business partners. For instance, such information could be posted at a visible location accessible to all such persons and on the website of the entity, and could also be included in courses and training seminars on ethics and integrity".

by the protective regime in one Member State but not in another). Information on which reports of breaches are protected should be tailored to the national transposition law of the Member State in which each company is located;

- second, as mentioned above, depending on how the national transposition law transposes the provision in Article 9(2), whistleblowers in a given Member State may have the right to request a physical meeting in the company with which they have a work-related relation;

- third, a given Member State may include more favourable provisions in its transposition laws (e.g. shorter deadline for acknowledgment of receipt or for feedback, rewards for whisleblowers, etc.), which are not the same in another Member State;

- fourth, rules on aspects of the internal reporting channels and procedures for follow up, such as on methods for providing feedback, could differ from one Member State to another depending on the national law of the Member State in which the company is located;

- fifth, differences in the organisation of internal reporting channels and procedures for follow up may also arise from one Member State to the other, as a result of the establishment of channels and procedures for internal reporting and for follow-up in consultation and in agreement with the social partners, where provided for by national law (Article 8(1)).

Within the framework of the requirements it imposes on private sector entities as regards the setting up of reporting channels, the Directive provides nonetheless for some flexibility on certain aspects.

First, pursuant to Article 8(5), "*reporting channels may be operated internally by a person or department designated for that purpose* ***or provided externally by a third party".*** According to the explicit wording of the Directive, this possibility refers to third parties that are *external* to the legal entity with which the reporting person has/had/is about to have a work-related relationship. As further clarified in Recital 54 *"Such third parties could be external platform providers, external counsel, auditors, trade union representatives or employees' representatives*". The third parties' role is limited to receiving the reports, and does not extend to giving follow up in terms of investigating and addressing the breach, where relevant (see Recital 54 "*third parties could also be authorised to receive reports of breaches on behalf of legal entities in the private and public sector, provided that they offer appropriate guarantees of respect for independence, confidentiality, data protection and secrecy"*). Thus, if a company chooses to outsource the operation of reporting channels to an external platform provider, for example, it will have to split the two functions: the external platform provider will be responsible for receiving the reports and acknowledging receipt within 7 days, whilst the designated person/department within the company will be responsible to diligently follow up on such reports and give feedback.

Second, mindful of the more limited resources of **medium-sized companies** (companies with 50 to 249 workers) and with a view to helping them meet their obligations under the Directive, the Directive (Article 8(6)) allows them to **share resources as regards the *receipt of reports* and *any investigation*** to be carried out. It should be underlined that the

responsibility to maintain confidentiality, to give feedback, and to address the reported breach remains, however, with each medium-sized company concerned. Only medium-sized companies can benefit from this possibility, **but this applies both to distinct companies with no link to each other and to companies that belong to the same group** (while being distinct legal entities).[2]

Third, based on Article 8(6), where in a given corporate group compliance programmes are organised at headquarters level, **it could be compatible with the Directive that a subsidiary company benefits from the investigative capacity of its parent company provided that:**

1) the subsidiary company is medium-sized (has 50 to 249 workers);

2) reporting channels exist and remain available at the subsidiary's level;

3) clear information is provided to the reporting persons as to the fact that a designated person/department at headquarters level would be authorised to access the report (for the purpose of carrying out the necessary investigation), and the reporting person has the right to object to that and to request that the reported conduct is only investigated at the level of the subsidiary;

4) any other follow up measure is taken and feedback to the reporting person is given at subsidiary level.

The rationale behind the third condition is that it must remain the whistleblower's choice whether to have his/her report handled only at subsidiary level (because, for example, s/he suspects the headquarters to be involved in the breach) or not. In fact, if this choice were not left in the hands of the whistleblower, s/he would directly turn to external reporting channels, thereby depriving the company of the chance to swiftly address the matter without incurring reputational and/or financial damage.

Fourth, in cases where the report reveals a structural problem or a problem that affects two or more entities of the group and that can only be effectively addressed with a cross-border approach that the subsidiary where the report was made has not the power to apply, to ensure the effectiveness of the Whistleblower Directive, **it would be compatible with its spirit that the person/department designated to maintain communication with the reporting person (Article 9(1)(c)) will inform him/her of such conclusion and ask for her/his agreement to report the facts to the company within the group which has such power, whilst recalling that if s/he does not agree to that, s/he in any case has the possibility to withdraw the report submitted internally and report externally to the relevant competent authority**. The duty of confidentiality under Article 16 will continue to apply.

---

[2] Examples of such pooling of resources and relevant good practices can be found in the Commission Communication accompanying the proposal for the Directive (Communication "Strengthening whistleblower protection at EU level", COM/2018/214 final) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0214

Fifth, it should be recalled that – as indicated in **Recital 55** – "*internal reporting procedures should enable legal entities in the private sector to receive and investigate in full confidentiality reports by the workers of the entity and of its subsidiaries or affiliates ('the group')*". This relates to cases **where persons working in a subsidiary would decide to report to the parent company of the group** (for instance because they feel safer or because they consider that the breach might be most effectively resolved by the parent company - e.g. it is not clear where the decision for the breach was taken/where the breach occurred, etc.). **In such cases, the parent company should accept and follow up on the report.**

This additional possibility given to the workers in subsidiaries cannot be turned into an obligation for them to report to the parent company. However, parent companies may decide to fully and systematically open their reporting channels to workers of their subsidiaries **An efficient information campaign within a group may actually result in workers naturally turning to the reporting channels of the headquarters**, except where they have specific reasons to have their reports handled *solely* by the subsidiary (for example, because they may fear retaliation from the parent company due to past cases of retaliation, whilst they do not perceive the same risk at the level of the subsidiary).

Finally, turning to the need to see through possible breaches across the group, to which you refer in your letter, it should be stressed that, even where the whistleblower objects to sharing the report with the headquarters, **the Directive does not prohibit sharing the *outcome* of a given case at group-level for instance** for ex-post auditing, compliance or corporate governance or other duly justified purposes, provided the confidentiality requirements laid down in the Directive are respected.

Turning to the concerns raised in the letter addressed by some Danish companies to the Danish Parliament, which you explicitly requested us to address in this reply, they seem to rest on a mistaken assumption: the Directive does not prohibit group companies from upholding a group whistleblowing function. The Directive requires that, where the group comprises entities with 50 or more workers, each one of them set up and operate its own internal channels (Article 8(3)). Where such central group whistleblowing function exists within a group, it will then be the whistleblower's choice to decide whether to report at that level or whether, given the specific circumstances of a given case, s/he prefers to report at the level of the subsidiary where s/he works. **A corporate policy instilling trust in the group whistleblowing function, possibly accompanied by an information policy publicising its availability and encouraging whistleblowers to report directly to the central group whistleblowing functions may result in whistleblowers tending to report there. However, the possibility to report to the subsidiary where the whistleblower works must remain effectively available**.

Having clarified that the Directive does not prohibit maintaining central whistleblower systems, the arguments under the two sub-sections in the letter do not hold.

With regard in particular to the arguments under the sub-section "a central whistleblower system secures consistent processing of whistleblower reports and whistleblowers across the group", it should be noted that such a consistent processing across the group aimed at ensuring the full respect of the requirements of the Directive could be achieved through appropriate "upstream" knowledge-sharing between group companies, relevant trainings and exchanges of good practices.

I hope the above clarifies.

Yours faithfully,

[redacted]