THE WHISTLEBLOWING DIRECTIVE

MORRISON FOERSTER

Nearly all EU Member States have now implemented the Whistleblowing Directive into their national laws. What does this mean for your company?

What is the Whistleblowing Directive?

- The Directive establishes a whistleblowing framework across the EU, requiring in-scope companies to set up whistleblowing hotlines/channels.
- The Directive contains minimum standards on how to respond to and handle concerns raised by whistleblowers. This means no full harmonization; whistleblowing rules therefore differ across the EU.

What violations may whistleblowers report?

- Any violation of EU law (including, but not limited to, violations regarding financial services, product safety, money laundering and terrorist financing, consumer protection, public health, data protection, and privacy).
- EU Member States have the option to extend this scope to other violations in their national laws.

What are the new compliance obligations?

- Your company must set up different channels so that reports can be received via post, telephone, physical complaint boxes, online forms, and in-person meetings.
- As long as they guarantee independence, confidentiality, data protection, and secrecy, third parties can also receive reports on behalf of your company.
- Receipt of each report must be confirmed within 7 days.
- Feedback about the findings or updates about the investigation must be provided to the individual within 3 months after receipt of the report.
- Note that certain EU Member States have deviated from these obligations and included additional requirements in their national laws.

Which companies need to comply?

- The Directive applies to companies with more than 50 workers.
- "Workers" is a broad term and may, for example, include regular employees, part-time workers, trainees/interns, and fixed-term contract workers.
- EU Member States may "encourage" companies with fewer workers to also establish a hotline.

Who is protected?

- All whistleblowers in the private/public sector who acquire information on violations of EU law in a "work-related context."
- This includes, for example, current and former employees, job applicants, subcontractors, shareholders, volunteers, interns, trainees, business partners, facilitators, colleagues, or relatives of the whistleblower who have a work-related connection with the whistleblower's employer, customer, or recipient of services.
- The motives of the whistleblower are irrelevant; they need only reasonable grounds to believe the violation (i) is true and (ii) falls within the reportable scope.

How are whistleblowers protected?

- All forms of retaliation are prohibited.
- EU Member States must ensure that whistleblowers have access to measures, such as protection from liability, financial assistance, psychological support, legal aid and advice, and protection in judicial proceedings.
- Under certain conditions, individuals can turn to external reporting channels (set up by each EU Member State) or, as a last resort, make a public disclosure.

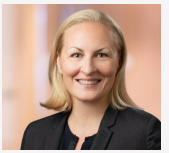
Visit MoFo's Whistleblowing Center for our latest resources to help you prepare.

How Can We Help You?

- A whistleblowing compliance program will need to be tailored to your company's profile. MoFo has extensive experience helping companies across different industries, including B2B and B2C organizations.
- We can work according to your specifications, whether on a national, pan-European, or global level.
- We can help you with every phase of preparedness, such as formulating and implementing your new compliance plan, preparing the relevant notices, documents, and agreements, and providing training for your staff.
- We would be delighted to discuss how we can assist with your company's specific needs.

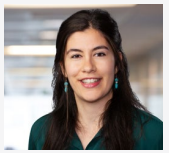
We're here to help. We're MoFo.

CONTACTS



Alja Poler de Zwart
Partner, Brussels
(32) 23407360
apolerdezwart@mofo.com

Dan Alam
Associate, London
(44) 20 7920 4113
dalam@mofo.com



Mercedes Samavi
Of Counsel, London
(44) 20 7920 4170
msamavi@mofo.com

Hanno Timner
Partner, Berlin
(49) 3072622-1332
htimner@mofo.com

Annabel Gillham
Partner, London
(44) 207 920 4147
agillham@mofo.com

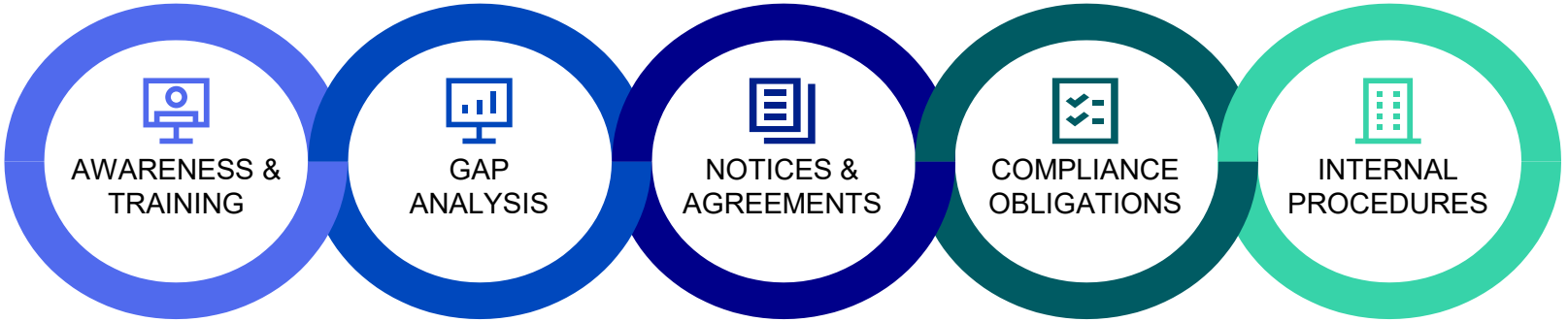
Alex van der Wolk
Partner, Brussels
(32) 23407369
avanderwolk@mofo.com

A PRACTICAL GUIDE TO YOUR OBLIGATIONS

MORRISON FOERSTER

The key tools that your company will need to build or update its whistleblowing compliance program

Whistleblowing Compliance Program



- Inform decision-makers in your company so they are aware that compliance with the Directive and local implementing laws is necessary
- Make sure your organization understands what this means for the company
- Educate and train key stakeholders (such as HR, Risk & Compliance, Privacy, and IT) on the relevant changes and next steps
- Consider that approval from or consultation with your works council/labor union may be needed

- Gauge what work needs to be done to meet the Directive's requirements, depending on whether or not you have an existing whistleblowing program
- Carry out a DPIA to review and mitigate potential risks with data processing activities under your whistleblowing program (or update the existent DPIA, as applicable)
- Monitor the implementation of the Directive in EU Member States relevant to your company, as well as any secondary legislation, regulatory directions and guidance, and consider how it impacts your whistleblowing program

- Update privacy notices and procedures to ensure sufficient information is provided to potential whistleblowers (and other implicated or otherwise involved individuals), also in accordance with the GDPR transparency requirements
- Ensure that compliant data processing agreements are in place with your whistleblowing service providers
- Verify that all relevant data transfer agreements or other transfer mechanisms comply with the EU transfer requirements

- Maintain your recordkeeping obligations under the Directive, local implementing laws, and Article 30 GDPR
- Conduct or update the hotline's legitimate interest assessment
- Check whether the hotline's technical and organizational security measures are appropriate
- Review and update your data retention policy to accommodate for personal information collected via the whistleblowing program
- Check that only limited staff and departments have access to the personal information
- Consider other relevant employment and privacy concerns; consult the relevant experts in your company

- Set up different channels (including in-person meetings) to receive reports directly from whistleblowers or via third parties, such as trade union reps
- Appoint a responsible person or department that can investigate in an independent and impartial manner, free from conflicts of interest
- Establish a process for acknowledging receipt of a concern and providing regular updates to the whistleblower
- Ensure that your whistleblowing process makes individuals comfortable using the hotline, so they do not have a reason to deviate towards external whistleblowing options (e.g., regulators or media)

Visit MoFo's Whistleblowing Center for our latest resources to help you prepare.

Specific Areas of Attention

- EU Member States have clarified certain concepts in their national laws. For example:
  - If anonymous reporting is permitted; and
  - If the scope of reportable concerns is broader.
- It is up to EU Member States to set national penalties for violations of the Directive, under their national laws.
- Remember that the GDPR and its penalty framework are also in play due to personal information being involved. This means all of your GDPR obligations will continue to apply.
- This is not just an EU concern. Other countries around the world (such as the UK, Japan, and the U.S.) either have existing laws or are in the process of introducing new or updated whistleblower laws.