Baker McKenzie.

EU Whistleblowing Directive

Act Now to make your Whistleblowing Program compliant

Q&As and the most common pitfalls to be avoided

December 2022

Investigations, Compliance & Ethics

CALIBRATE RISK GLOBALLY

Frequently asked questions regarding the EU Whistleblowing Directive

We have an effective whistleblowing program in place – does that mean, we do not have to change it?

Even if you have a sophisticated and effective whistleblowing program in place, it is almost certain that the EU Whistleblower Directive ("WBD") and the implementation laws in the EU Member States will require you to adjust it. Depending on the current setup, minor adjustments may suffice. But in some cases, significant adjustments need to be implemented that affect the setup of the global whistleblowing program.

Why do we need to adjust our whistleblowing program?

The aim of the WBD and the implementation laws in the EU Member States is to protect whistleblowers. The WBD is intended to establish uniform minimum standards throughout the EU to ensure effective whistleblower protection (focus on the whistleblower). The WBD is not a blueprint for an effective whistleblowing program. It only dictates the requirements companies need to implement to protect whistleblowers when reporting misconduct. In fact, some of the requirements may render the existing whistleblower programs less effective. Lastly, adjusting the existing whistleblowing program to the WBD often means that the data protection measures need to be revised as well.

What happens if we do not act?

As with every modern compliance legislation, violating the WBD and its implementation laws may lead to fines, in particular, if a company fails to protect the confidentiality of a whistleblower or if they are retaliated against. Unlike other laws, the fines are monetary values and not calculated based on a percentage of the companies' turnover. But since there is no central authority to monitor the implementation across the EU, companies may be scrutinized by up to 27 Member States.

In addition to the sanctions under the WBD and implementation laws, companies may violate data protection requirements and rights of affected individuals under the GDPR. And the consequences for data protection violations may be significantly more severe for multinationals operating in the EU.

Is the WBD in force yet?

The WBD itself is in force, but it only binds the Member States. They were obliged to transpose the WBD into national legislation by the end of 2021. But only 10 out of 27 have passed national implementation laws as of 1 November 2022. Of the larger countries, France, Sweden and Portugal have already implemented the WBD. The German implementation law is in its final stages. Italy, Spain, the Netherlands, Belgium and Poland are also refining their draft implementation laws.

How much time do we have left to implement the adjustments?

In Member States that have already implemented the WBD, companies must follow the existing requirements. The current draft laws usually contain a grace period of up to three months. But since the necessary changes may require significant adjustments and involvement of multiple stakeholders, companies should act swiftly.

Do we need to implement 27 different whistleblowing programs?

The aim of the WBD is to introduce an EU-wide concept to protect whistleblowers. This means in practice that companies may implement a homogeneous whistleblowing program in the EU, while observing special national law requirements. Additional complicating factors are statements from the EU Commission requiring companies to implement local whistleblowing channels (cf. section I.3. below). Companies should also check whether adjustments to the whistleblowing program trigger any co-determination or information rights of works councils.

Common issues and pitfalls

Protection mechanisms and procedural aspects of the WBD and national implementation laws

1. Do you allow employees to submit reports to other functions, e.g., managers, HR, legal, audit?

This is one of the most crucial issues: If you offer a variety of formal whistleblowing channels, each channel has to satisfy all applicable procedural requirements (e.g., documentation, confidentiality, independence, etc.). If the number of the whistleblowing contacts that employees can submit complaints to is relatively large, ensuring confidentiality, proper documentation, independence and sufficient expertise of these whistleblowing contacts is costly, burdensome or even practically impossible, exposing the company to fines under the WBD/implementation laws.

2. Are the whistleblowing channels available to all individuals concerned?

Some national implementation laws extend the scope beyond a single group of individuals such as current employees. Some national laws, for example, the German Supply Chain Act, require companies to make a whistleblowing channel available to third parties outside the organization. Under the German Supply Chain Act, the whistleblowing channels need to be available to any person in a given company's supply chain.

3. Does your reporting channel offer employees the option to report to local whistleblowing contacts ?

In practice, multinational companies have established group-wide, central whistleblowing channels. The complaints are usually handled by specialized teams in designated hubs. However, the EU Commission (and some EU national legislatures) issued statements that it prefers companies to have a dedicated whistleblowing program in each legal entity of a group of companies. It will likely take some time to settle this dispute between the EU Commission and the Member States. But companies should, in any case, take preliminary steps to at least give their employees the option to report an issue locally, e.g., via adding an option to the whistleblowing platform that routes the complaint to the local Whistleblowing Team.

4. Have you organizationally ensured that the Whistleblowing Team operates independently and has sufficient expertise?

The WBD requires the Whistleblowing Team to operate independently, i.e., it must not be bound by instructions from other functions in the company when reviewing complaints. This needs to be established on an organizational level.

5. Is your confidentiality concept audit-proof?

Confidentiality is a key feature of the WBD to protect whistleblowers from retaliation and to ensure that allegations can be investigated without interference from affected individuals. For this reason, confidentiality violations are punishable offenses in the EU.

Confidentiality needs to be organizationally ensured via robust controls throughout the entire life cycle of a report, from the moment the report is submitted (Who is able to see the report? Is the identity of the whistleblower shared with other functions, e.g., management, without their consent?). In addition, confidentiality extends to other individuals beyond the whistleblower.

It is particularly burdensome for a company to ensure confidentiality in an auditable way if reports may also be submitted to individuals outside a (central/local) Whistleblowing Team (see section 1. above), like management, HR, etc. Without strict procedural rules, it often cannot be ensured that only authorized persons learn about the subject of the report, the identity of the whistleblower and other individuals concerned.

Lastly, companies are confronted with a dilemma under the WBD, because they must protect the identity of a whistleblower but also ensure that allegations for retaliation are investigated properly. This task can practically become challenging.

6. Is your retaliation protection limited to the whistleblower?

Just like confidentiality, the prohibition of retaliation is at the heart of the WBD, and the national implementation laws and violations may lead to significant fines. The protection mechanism is not limited to the whistleblower. It also protects other individuals, e.g., individuals who supported the whistleblower or assisted during an investigation.

7. How do you ensure retaliation protection and protect the company in case of retaliation allegations?

Managers and HR need to be aware of the prohibition to retaliate and understand their responsibility to stop, address and prevent retaliation. This can be achieved by way of trainings and by holding those accountable who engage in or fail to stop retaliation. To be best protected in case of unfunded retaliation allegations, managers and HR should document the underlying reasons for HR decisions.

EU data protection

1. Have you assessed the data processing justification, in particular, for report outside the scope of the WBD and national implementation laws?

Any processing of personal data requires a legal basis. Whistleblowing reports generally contain personal data of the whistleblower as well as the other individuals affected.

To the extent there is no legal obligation that requires the processing of personal data, another justification to process the data must be established and documented.

This applies, for example, to alleged violations that do not fall under the scope of the WBD and implementation laws. Companies usually tend to apply a broad scope to their whistleblowing concept, covering apart from criminal conduct, violations of laws applicable to the company and violations of internal policies. However, the scope of the WBD and implementation laws is narrower. It does not cover violations of internal policies and the scope is often limited to severe violations of laws.

2. Have you considered and taken data protection measures regarding the whistleblowing program?

There are several measures that need to be considered and adopted from a data protection law perspective when implementing or adapting a whistleblowing program. The following is a non-exhaustive selection of typical measures (the details depend on the specific set-up): data protection agreements, involvement of data protection officer, notice to employees and other individuals who shall be permitted to submit reports, notice to affected individuals, manual/instructions for individuals who review and further investigate the reports, records of processing activities, intra-group data protection agreements, data protection impact assessment, deletion concept, data security concept, additional local law requirements and specifics.

3. Are you prepared for Data Subject Access Requests ("DSAR")?

DSARs have become challenging tools, particularly popular with individuals subject to whistleblowing reports. The scope of the DSAR is broad and companies may be confronted with a request to disclose information about a complaint or an investigation. At the same time, they must ensure confidentiality and protect the whistleblower and others (see section I.5. and 6. above) from retaliation. The WBD and the national implementation laws provide little guidance on how companies should handle such situations. It has proven to be helpful in establishing standardized processes to ensure that the company responds to DSAR in a consistent and coordinated manner and takes the associated risks in all directions into account by carrying out a case-by-case assessment – also considering local (data protection) laws.

Effectiveness

Whistleblowing programs must be compliant and effective

Compliance with the requirements of the WBD and national implementation laws as well as data protection requirements are regulatory requirements. But companies must also ensure that the whistleblowing program is effective. A whistleblowing program is **effective** if:

- whistleblowers are encouraged to report misconduct,
- the reporting channels are user-friendly,
- the reports are processed promptly and properly,
- the reports are handled consistently and equally,
- the necessary follow-up measures, in particular internal investigations, are initiated when adequate,
- sanctions are imposed and corrective measures are taken where suspicions are confirmed, and
- the entire process is established in an auditable way.

CONTACTS:

Dr. Nicolai Behr
Partner
+49 89 5 52 38 204
nicolai.behr@bakermckenzie.com

Dr. Michaela Nebel
Partner
+49 69 2 99 08 368
michaela.nebel@bakermckenzie.com

Dr. Robin Haas
Counsel
+49 89 5 52 38 227
robin.haas@bakermckenzie.com

Katja Häferer
Partner
+49 69 2 99 08 277
katja.haeferer@bakermckenzie.com

Margarita Fernandez
Partner
+34 91 230 45 79
margarita.fernandez@bakermckenzie.com

Monica Kurnatowska
Partner
+44 207 919 1870
monica.kurnatowska@bakermckenzie.com

Ester Maza
Partner
+34 91 391 51 89
ester.maza@bakermckenzie.com

Julia Wilson
Partner
+44 207 919 1357
julia.wilson@bakermckenzie.com

Joanna Ludlam
Partner
+44 207 919 1822
joanna.ludlam@bakermckenzie.com

Christoph Kurth
Partner
+41 44 384 13 00
christoph.kurth@bakermckenzie.com

Florian Tannen
Partner
+49 89 5 52 38 112
florian.tannen@bakermckenzie.com

CALIBRATE RISK GLOBALLY

Whether dealing with high-stakes investigations, defending against government enforcement actions, or pursuing growth opportunities, success depends on calibrating risk. With highly skilled lawyers on the ground around the world, we understand the regulatory, business and cultural landscape, wherever you are. And by connecting investigations and rapid crisis response with effective risk management solutions, our integrated approach helps you safeguard your business and protect corporate reputation.

bakermckenzie.com