NAVEX™

Solutions Guide

EU Whistleblower Protection Directive

How Can NAVEX Help You Comply?

What is the EU Whistleblower Protection Directive?

Directive (EU) 2019/1937, commonly referred to as the EU Whistleblower Protection Directive or the EU Whistleblowing Directive, ("the Directive") was adopted by the European Council in 2019. It aims to strengthen protections for people who report breaches of EU law, create safer, better-defined reporting channels across all EU member states, and move member states towards a unified legal framework.

The Directive has implications for hundreds of thousands of organizations within the EU – and beyond. December 2021 marked the deadline for member states to enact national law satisfying the requirements of the Directive for organizations of 250 people or more, leaving two further years for smaller organizations of 50 or more people. Note that laws will vary by country, as the Directive establishes minimum standards, which will be transposed to national law in each member state.

What are the benefits of complying with the Directive?

Beyond the legal requirements established in the legislation, research suggests there are real benefits to organizations that encourage internal reporting. A recent George Washington University study showed that higher organizational whistleblowing rates correlate to decreases in material lawsuits, settlements, and negative news stories[1]. Low reporting numbers rarely indicate a lack of misconduct in an organization. Rather, unreported concerns represent a serious risk, creating organizational blind spots that can become glaring (public) crises if left unresolved.

An effective, trusted avenue for employees and affected parties to report allegations of wrongdoing is fundamental to creating a more ethical culture in any organization. Beyond empowering and protecting individuals who choose to speak up, the insight gained through a mature incident management program can be hugely beneficial to organizations of any size. The knowledge collected from whistleblowing can be used to identify areas of organization risk, inform and enhance internal training programs, and modify policies to encourage more positive operational outcomes.

[1] George Washington University, Evidence on the Use and Efficacy of Internal Whistleblowing Systems, 2018

Does our current governance, risk and compliance (GRC) program align with the Directive?

While legislation will vary at member state level, the Directive establishes several fundamental minimum requirements organizations must satisfy. NAVEX offers a range of solutions designed to help you meet the requirements laid out in the Directive:

Whistleblower Protection Directive Requirement	NAVEX Platform Features
Provide safe, accessible channels to report incidents to the organization. Whistleblowers should be able to submit reports orally, in writing, and/or in person.	NAVEX solutions establish a central repository for reports from multiple channels. The continuing upward trend in non-telephonic reporting reinforces the need for varied, visible, accessible channels for whistleblowers within and outside of an organization. NAVEX solutions capture web, telephone, mobile and in-person reports.
Maintain confidentiality for the whistleblower, the person named in the report, and any third parties referenced.	In addition to secure anonymous reporting capabilities, NAVEX incident management platforms are designed to help you comply with the strict data privacy protections established in the GDPR. NAVEX offers secure data storage in a data center located within the EU. Company-wide information security measures ensure confidentiality is maintained at data centers within and outside of the EU. Audit logs are created by and stored within the application database. These contain events such as logins and actions taken with each report (case creation upon report submission, updates, etc.). These are available to the customer for the life of the contract from within the application.
For telephonic reports, reporting person must be given the opportunity to check, rectify, and agree to the transcript of the call by signing it.	NAVEX contact center agents read back the report to the reporter before submission, providing the reporter with the opportunity to modify and verify the contents of the report. Reporters are also provided a report key and instructions for how to follow up within the EthicsPoint system. Once the report is in the system, the reporter may log in and review the written report and post any additional comments, including comments correcting or supplementing the report. Alternatively, customers can download a copy of the report and transmit it to the reporter for signature in whatever medium is desirable (e.g., EchoSign, fax, overnight courier, etc.). Customers can utilize the follow-up tool in the system to facilitate any conversations and attachments, as appropriate.
Acknowledge receipt of reports within seven days.	Prompt report response times are driven by an efficient program structure. NAVEX incident management solutions enable automated alerts and processes to assure reporters their case has been received and is being processed. There is also an option to enable a feature called "Automated Reporter Follow-up," which is a customizable follow-up message posted to the report that the reporter can login and view.
Respond to and follow up on reports within three months, define and detail the investigation and decision-making process.	With NAVEX, organizations can use fully configurable role- and rule-based routing and automated workflows to streamline reporting structures and processes, helping keep cases moving and providing timely feedback to interested parties. Default and customizable reminders can be set for reporter follow-up. Our EU Whistleblower course, part of NAVEX's training curriculum, covers best practices and expectations for managers handling and escalating reports to give their employees confidence in the reporting process.

Whistleblower Protection Directive Requirement	NAVEX Platform Features
Maintain auditable reporting records while adhering to data protection rules.	The comprehensive, searchable, secure collection of reports and reporting data created with a NAVEX incident management platform is an invaluable resource for auditors, investigators, and authorities and acts as a crucial safety net for organizations before, during and after an incident. GRC Insights, NAVEX's compliance benchmarking and analytics tool, is designed to deliver a holistic view of your risk and compliance reporting data and deliver custom dashboards to drive program performance and inform strategic business decisions, creating deep operational and cultural value for the organizations that use it.
Protect whistleblowers against dismissal, demotion and other forms of retaliation.	NAVEX helps organizations create clear, auditable, thoroughly documented report management processes to help prevent and/or identify any potential retaliatory activity against whistleblowers. Encouraging reporting and protecting whistleblowers from retaliation goes beyond incident management. Organizations should develop, implement and maintain effective policies and processes that will protect employees from retaliation. Policy and procedure management is key for distribution and attestation. A well-formed, broadly accepted code of conduct helps give employees the confidence to speak up. NAVEX's EU Whistleblower Training course provides employees and managers training on best practices for reporting and how to identify and prevent retaliatory actions.
Localize reporting within separate legal entities; provide reporters with control over who has access to their report and how it is investigated.	NAVEX enables fine control over report intake, shared investigative resources, and outcome sharing for the purpose of ex-post auditing, compliance, or corporate governance. Depending on an organization's structure, NAVEX incident management solutions can be implemented using multiple hotlines, web and mobile intake sites to establish dedicated intake channels for separate legal entities. Intake processes for both web-based and telephonic channels can be augmented to support automated report acknowledgment, reporter consents, and the option to check/rectify/sign a submitted report. Customizable access tiers help customers control user access to report data to ensure confidentiality requirements are upheld. Rules regarding inter-country report and resource sharing may be affected by state-level transpositions, which are still developing. For more details on localized reporting, please refer to our [Transposition Tracker].
Provide workforce with appropriate information on the existence and proper usage of reporting channels.	Customers can customize their notice and consent statements to provide appropriate information on internal reporting procedures as well as on external reporting procedures to relevant competent authorities, as required by the Directive. NAVEX provides courses to train employees on best practices and procedures for raising concerns, the importance of utilizing internal channels, when and what to report and what to expect through the reporting process.

Whistleblower Protection Directive Requirement	NAVEX Platform Features
Provide access to reporting channels for third-party networks to report breaches within the context of doing business.	NAVEX incident management solutions encompass a broad collection of channels that can be made available to parties operating externally or tangentially to an organization. Training and awareness programs can be designed to include third-party networks and encourage broad knowledge of where to find and how to use appropriate reporting channels, and the extended protections from retaliation afforded therein.
Ensure impartiality and competence of the people managing the reporting channels and handling the reports.	NAVEX's incident management solutions make it possible to assign individual cases to specific stakeholders, including outsourcing or third-party management where allowed.

Frequently Asked Questions

What if we operate in multiple EU Member States?

According to the text of the legislation, there is no legal basis requiring separate, dedicated whistleblower setups in each affected country. Dedicated reporting channels, report and resource sharing, and responsibilities of acknowledgment are instead dictated by an organization's structure, determined primarily by legal entity size(s). If member state legislation arises that does create a basis for this requirement, NAVEX enables you to create multiple intake systems customized by geographic location and/or subsidiary.

Does my whistleblower reporting system comply with data privacy legislation?

Depending on where you operate, the data associated with your incident management system is likely governed under one or many overarching data privacy regulations. NAVEX's incident management solutions are tailored to help you satisfy both GDPR requirements and national data protection laws.

How is anonymous reporting handled?

While provisions regarding anonymous reporting vary across member states, NAVEX's incident management solutions support anonymous reporting and case management where appropriate. While we have seen a steady decline in overall anonymous reporting across the industry over the past decade[2], the ability for whistleblowers to report and follow up on allegations anonymously remains a valuable tool in the compliance arsenal. Technological considerations such as anonymized reference coding, in-app messaging for anonymous reporters, and GDPR-compliant data privacy practices promote safety and trust for whistleblowers who decline to identify themselves.

This is a directive, not a regulation; what will the effect be for my organization/state?

While this document pertains to the specific requirements laid out in the text of the Directive (rather than specific legislation), the Directive will have a direct effect in each member state. Member states are still in the process of transposing the Directive into national law. The resulting laws will be legally enforceable at member state level from the date of their enactment. We are closely monitoring the transposition process across all EU countries; for country-specific details please refer to our [Transposition Tracker].

2 Penman, Carrie. "Risk & Compliance Incident Management Benchmark Report," NAVEX Global, 2021, p. 7.

Will legal implementation differ among EU states?

The Directive seeks to establish a unified framework and legal standard across all member states. As each member state must transpose the Directive into national law, the states will have control over how individual aspects are applied at a local level. Some member states may extend their transposition to encompass a broader scope or stricter standards—this is allowable if their implementation meets or exceeds the minimum standard established in the Directive.

Will there be additional requirements in my country?

Member state transpositions may result in expanded legal requirements at the national level. For example, Sweden's proposal covers reported breaches of not just EU law (the minimum standard), but also Swedish national law. Aspects such as types of misconduct reported and whether reports have been submitted anonymously may also see some disparity in the qualification for protection in different member states. Deterrents, such as financial or legal penalties for those organizations or persons that breach the new rules, will similarly be set at member state level and are likely to produce some divergence across the 27 member states.

With many member states yet to establish final transpositions of the Directive, the full extent of the differences will only become clear as those national laws are proposed, defined and enacted.

Can I do more to encourage ethical behavior in my organization?

An incident management platform serves as a valuable foundation for any risk and compliance management program. The reports captured through these channels constitute a wealth of information and can provide your leaders valuable insight into the health and wellbeing of their organization, its structures, and everyone directly involved in your operations.

Organizations that use whistleblowing and speak-up programs to feed into their larger compliance framework see benefits in deeper insights and stronger workplace culture. NAVEX offers a comprehensive ecosystem of solutions and products that work in concert with your organization's whistleblowing program.

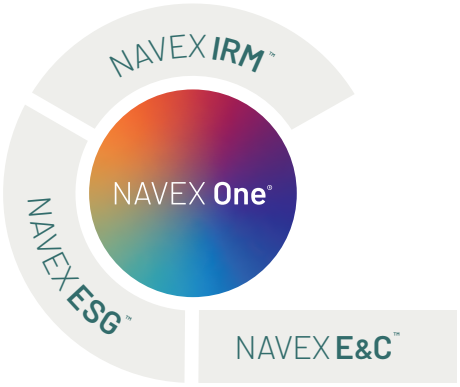
First, all ethics and compliance programs should be underpinned by a strong code of conduct. This document should function as a thoughtful expression of an organization's values, and reinforce the fact that employees are encouraged to speak up when they see something wrong.

Robust training programs act as a strong foundation for promoting a speak-up culture when paired with whistleblowing programs. Training programs teach employees best practices, highlight real-world examples of sometimes complex issues, and show employees that their organization takes unethical behavior seriously.

Training and enforcement of your organization's values is a continuous process. Many organizations employ a comprehensive, programmatic policy management system to effectively update, communicate, and distribute their internal policies among a varied collection of stakeholders. Centralized repositories and digital distribution systems provide employees easy reference while providing organizations with an auditable attestation record.

When implemented thoughtfully and maintained effectively, these systems work together to foster a more ethical organizational culture.

To learn more about the details and implications of the EU Whistleblower Protection Directive, please visit our site, or contact us to discuss the details of your organization's ethics and compliance program.



NAVEX **E&C** Solution is part of NAVEX **One**®

- Incident Management
- Ethics & Compliance Training
- Policy & Procedure Management
- Code of Conduct