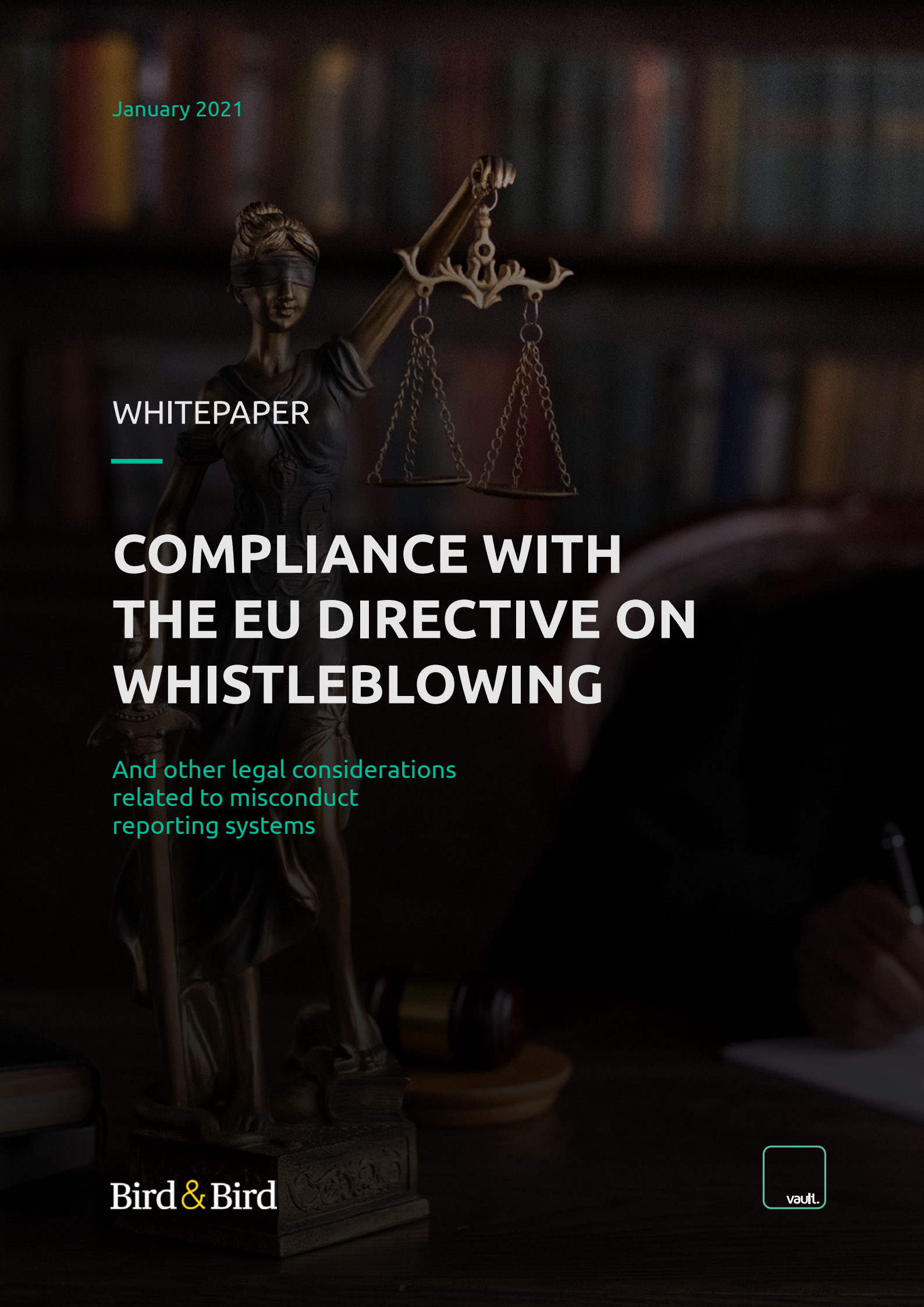
January 2021



WHITEPAPER

COMPLIANCE WITH THE EU DIRECTIVE ON WHISTLEBLOWING

And other legal considerations related to misconduct reporting systems

Bird & Bird

vault.

Table of Contents

01

Introduction

Persons who work for a public or private organisation or are in contact with such an organisation in the context of their work-related activities are often the first to know about threats or harm to the public interest which arise in that context. By reporting breaches of Union law that are harmful to the public interest, such persons act as 'whistleblowers' and thereby play a key role in exposing and preventing such breaches and in safeguarding the welfare of society. However, potential whistleblowers, whether reporting internally to stakeholders within their organisation or to an external body such as regulator or the Ombudsman, are often discouraged from reporting their concerns or suspicions for fear of retaliation. In this context, the importance of providing balanced and effective whistleblower protection is increasingly acknowledged at both Union and international level.

On 7 October 2019, the Council of Ministers of the EU therefore adopted a new whistleblower Directive (the **"WB Directive"**), which must be implemented in the EU member states no later than 17 December 2021.

According to article 1, the purpose of the Directive is to enhance the enforcement of Union law and policies in specific areas by laying down common minimum standards providing for a high level of protection of persons reporting breaches of Union law.

Whilst December 2021 may still feel like a long way off, international businesses (particularly those with operations in a large number of EU jurisdictions, where the time needed to agree changes to policies and then translate these can be significant) can avoid a last-minute rush to compliance by preparing now to:

- Review their standards of business conduct and reporting arrangements, including internal whistleblower solutions or reporting systems, to ensure compliance with the Whistleblowing Directive and continued compliance with GDPR; and
- Implement internal whistleblowing policies (or adapt their existing policies to ensure they take account of the new legislation).

The WB Directive obliges both companies (with more than 250 employees from 2021 and more than 50 employees from 2023) and authorities in general to introduce whistleblower schemes, which must be available to all employees in the company/authority. With the new WB Directive, it is also possible that the scheme also influences external partners, e.g. clients or consultants.

The scheme can be established in various ways, i.e. in writing and submit reports by post, by physical complaint box(es), or through an online platform, whether it be on an intranet or internet platform, or to report orally, by telephone hotline or other voice messaging system, or both. The online platform is expected to be the most common way of implementing the requirement for a whistle blower scheme.

According to the WB Directive premise (33):

> Reporting persons normally feel more at ease reporting internally, unless they have reasons to report externally. Empirical studies show that the majority of whistleblowers tend to report internally, within the organisation in which they work.
>
> Internal reporting is also the best way to get information to the persons who can contribute to the early and effective resolution of risks to the public interest (…)

To embrace this opportunity inside Europe, an online platform (as well as any other scheme established) must follow the rules and requirements laid down in the WB Directive and in relation to the processing of data in accordance with General Data Protection Regulation (GDPR).

The WB Directive sets up requirements to the WB scheme to be put in place. Some of these are mandatory and must – as a minimum – be implemented in the specific jurisdiction and thus in the system used. Some of these are, however, also considered as guidelines, but recommended implemented in the system.

> This white paper has been prepared by Vault Platform, a digital platform for misconduct reporting in the workplace, and the law firm Bird & Bird.
>
> The aim is to inform HR, compliance and legal professionals about the requirements under the upcoming WB Directive, and to outline how Vault Platform enables public and private companies to meet these key regulatory requirements in relation to the establishment of an internal reporting platform.

Topics covered in this white paper include:

- An overall description of the WB Directive.
- A description of the process through which the reporting takes place and actions being taken etc.
- How Vault Platform enables compliance with the various requirements under the WB Directive.
- How Vault Platform deals with the rights of individuals who report via the Platform.

At the conclusion of this white paper the reader will have a good overview of all important aspects of the WB Directive, and considerations when using an online platform for compliance purposes, such as Vault Platform.

However, please also note that many aspects of the regulation are specific to territory and that the requirements stipulated in the WB Directive may be extended or changed when implemented in the EU member states.

02

An Overall Description of the WB Directive

As stated, the Directive applies to private companies with 250 or more employees from 2021, and 50 or more employees from 2023. However, this threshold does not apply if there is an obligation to establish a whistleblower scheme under other special legislation, including financial services regulations or the money laundering regulations. As a rule, all public authorities must establish an internal whistleblower system.

2.1. Three tier requirements for reporting

Under the Directive, a three-tier reporting structure is being introduced whereby employees can report their concerns through:

1. Internal reporting channels: facilitated by the organisation either through own developed channels or supplied by external providers (such as Vault Platform). Reporting through internal channels will be directed to an internal dedicated team.

2. External reporting channels: facilitated by the relevant national authorities or the appropriate EU institutions. Reporting through external channels will be directed to the designated authorities.

3. Public reporting channels: such as going directly to the media, or a public forum such as Twitter.

The WB Directive premise (47) states that:

> **"For the effective detection and prevention of breaches of Union law, it is vital that the relevant information reaches swiftly those closest to the source of the problem, most able to investigate and with powers to remedy it, where possible.**
>
> **As a principle, therefore, reporting persons should be encouraged to first use internal reporting channels and report to their employer, if such channels are available to them and can reasonably be expected to work. That is the case, in particular, where reporting persons believe that the breach can be effectively addressed within the relevant organisation, and that there is no risk of retaliation.**
>
> **As a consequence, legal entities in the private and public sector should establish appropriate internal procedures for receiving and following up on reports. Such encouragement also concerns cases where such channels were established without it being required by Union or national law.**
>
> **This principle should help foster a culture of good communication and corporate social responsibility in organisations, whereby reporting persons are considered to significantly contribute to self-correction and excellence within the organisation."**

This development is partly driven by ineffective incumbent internal whistleblowing mechanisms (such as 'hotlines') which frustrate potential reporters and drive them to other avenues. In this regard the WB Directive means businesses will have a greater responsibility to ensure internal reporting mechanisms are up to scratch, moving away from 'best-effort' solutions towards more appropriate, efficient and effective reporting channels.

From the perspectives of both business benefits and organisational culture, having prospective whistleblowers use an internal reporting channel first is by far the most desirable approach. Not only does this minimise the risk of financial and reputational damage of an incident going public or to the courts, it also strengthens trust between the employee and employer even to the point of encouraging more people to speak up before concerns boil over.

Also, third parties could also be authorised to receive reports of breaches on behalf of legal entities in the private and public sector, provided they offer appropriate guarantees of respect for

independence, confidentiality, data protection and secrecy. Such third parties could be external reporting platform providers, external counsel, auditors, trade union representatives or employees' representatives.

Finally, such an environment sets an example that misbehaviour of any kind will not be tolerated and employees are encouraged to report diversions, making potential corruption or ethical breaches less attractive to perpetrators.

External whistleblower channels are thought to supplement internal channels. The WB Directive thus requires that both internal and external channels are established, meaning that the fact that member states will comply with this obligation by establishing external channels does not exempt businesses from their obligation to set up internal channels.

2.2. The material scope of the Directive

The WB Directive lists in Article 2 the "material scope" of the Directive, i.e. what types of reports of breaches of EU law in principle will fall within the scope of the Whistleblower Directive. In other words; the types of reporting categories which will protect the person reporting under the Directive and require the internal reporting mechanism to serve. The material scope includes:

i. Public procurement;

ii. Financial services, products and markets, and prevention of money laundering and terrorist financing;

iii. Product safety and compliance;

iv. Transport safety;

v. Protection of the environment;

vi. Radiation protection and nuclear safety;

vii. Food and feed safety, animal health and welfare;

viii. Public health;

ix. Consumer protection;

x. Protection of privacy and personal data, and security of network and information systems;

The new Directive does not provide a completely new form of protection, e.g. there is also a requirement for whistleblower schemes in financial services today. The main difference is that the WB Directive will impose an obligation to set up whistleblower schemes to a much wider group of enterprises than before, regardless of the type of business one has and regardless of whether the companies are necessarily engaged in the core of the listed material applications.

However, in the context of the implementation process, member states may extend the scope of what can be reported, i.e. extending the scope of protection for the person reporting. In fact, the EU Commission encourages Member States to go beyond this minimum standard and establish comprehensive frameworks for whistleblower protection based on the same principles.

Therefore it would be important and interesting to track to what extent Member States may choose to include reporting on breaches of other sets of legislation under the implementation legislation. Obvious elements to consider would be workplace harassment and discrimination along with various types of misuse of governmental/ public funds, including i.e. bribery, which are not directly covered by the Directive. In any case Vault Platform will cover such additional implementation for each member state.

The Directive was approved in October 2019 with the intention of granting greater protection for those who seek to expose corporate wrongdoing. One of the unintended consequences of this move however, will be to encourage whistleblowers to report misconduct to external bodies in the first instance. It is therefore in the strongest interest of businesses to establish a trusted mechanism internally to encourage internal whistleblowing as opposed to external.

2.3. Requirements of the reporting channels

According to the Directive, it is up to the relevant Member State to define how to establish the necessary whistle blower channels as long as the relevant potential whistleblowers' identities are ensured to be kept confidential.

The authority/company must ensure that some minimum requirements in the Directive are followed, e.g. that:

- The channel is designed, established and operated in a secure manner that ensures the confidentiality of the reporting person's identity and that any third party mentioned in the reporting is protected, and that prevents unauthorised employees' access to it (WB Directive art. 9(1)a and premise (76));
- A confirmation of receipt of the report is given to the reporting person within seven days;
- An impartial, competent person or department is appointed to follow up on the reports. This person or department must maintain communication with the reporting person and, where necessary, request further information from and provide feedback to this reporting person;
- A careful follow-up is carried out on the designated person or department (The choice of the most appropriate persons or departments within a legal entity in the private sector to be designated as competent to receive and follow up on reports depends on the structure of the entity, but, in any case, their function should be such as to ensure independence and absence of conflict of interest. In smaller entities, this function could be a dual function held by a company officer well placed to report directly to the organisational head, such as a chief compliance or human resources officer, an integrity officer, a legal or privacy officer, a chief financial officer, a chief audit executive or a member of the board.);
- A reasonable time limit is set for giving feedback which does not exceed three months from the acknowledgment of receipt

or, if no acknowledgment was sent to the reporting person, three months from the expiry of a period of seven days after the alert was given (Where the appropriate follow-up is still being determined, the reporting person should be informed about this and about any further feedback to expect); The channel contains clear and easily accessible information on the procedures for making reports externally to competent authorities, see the WB Directive art. 9(1)g and premise (89) (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).

In addition, the Member States may add more procedural rules when implementing the Directive.

2.4. Protection from reprisals

The WB Directive states that protection should be granted to persons who provide information necessary to detect infringements which have already taken place, infringements which have not yet taken place but which are likely to take place, as well as acts or omissions which the reporting person has reasonable cause to regard as violations, as well as attempts to conceal violations. It is therefore not necessarily a requirement that an infringement has taken place or will take place, as long as the person reporting had a reasonable reason to believe that this was the case.

Thus, article 6(1)(a) of the Directive states that reporting persons are protected provided that “they had reasonable grounds for believing that the information provided on infringements was correct at the time of the notification and that such information was covered by this field of application".

The Directive states that the requirement is “an important protection against malicious, junk or unreasonable reporting, as it ensures that persons who intentionally and knowingly reported incorrect or misleading information at the time of reporting do not enjoy protection". Conversely, the Directive also states that it will, however, be “justified to protect persons who do not provide actual evidence but raise reasonable doubt or suspicion. At the same time, however, protection should not include persons who report information that is already fully available to the public or in the form of unfounded rumours and gossip”. In other words, it may very well be difficult to assess whether there was such a “reasonable reason" for the report.

Furthermore, the Directive also states that “*the motives of the reporting agents to report should be irrelevant as to whether they should be protected"*. It is clear that a motive should not in itself be decisive, but it is probably difficult not to attach any weight to this in the assessment of whether the person also had a “reasonable reason" to assume that the relationship was correct. Thus, if the motive was solely to harm the person being reported, for example, that the reporting person does not like the person (e.g. boss) being reported and there is evidence / indication of this on the basis of previous cases, it may thus support that the report has the character of unfounded rumours and gossip and that there was therefore no “reasonable reason”. The motive can therefore hardly avoid being given at least some weight in the assessment of whether there is a “reasonable reason".

Provided that such “reasonable grounds” are present, the WB Directive premise 40 states that:

> “Effective whistleblower protection implies protecting also categories of persons who, whilst not relying on their work-related activities economically, can nevertheless suffer retaliation for reporting breaches. Retaliation against volunteers and paid or unpaid trainees could take the form of no longer making use of their services, or of giving them a negative employment reference or otherwise damaging their reputation or career prospects.”

Thus, the main scope of the Directive is to prohibit Member States and employers from any form of reprisal against whistleblowers as a whistleblower might be intimidated from making a report if this is the case. This is stipulated in Article 19.

Such reprisals include suspension, termination, demotion or failed promotion, pay reduction, change in working hours, coercion, harassment or exclusion in the workplace etc. and applies to both employees, consultants, and suppliers etc.

The whistleblower is only protected from those reprisals if the whistleblower had reasonable grounds to assume that the relevant information was true and correct and that the reporting related to breaches (of EU legislation) that fell within the scope of the Directive at the time of the reporting.

On this basis, if a whistleblower is exposed to such reprisals after making a report (coved by the scope of the Directive), it will be assumed that the reprisals are initiated due to the report and the employer must in this case prove that the reprisals were not initiated due to report. This will be a heavy burden of proof to lift by the employer, and expectedly it will be rather similar to the protection currently found in the EU based anti-discrimination and equal treatment legislation.

Finally, article 21 of the WB Directive supports that the Member States shall take the necessary measures to ensure that whistleblowers are protected against retaliation. Such measures shall include, in particular, those set out in paragraphs 2 to 8 of the Article 21. This among others, include, that where persons report information on breaches or make a public disclosure in accordance with the Directive they shall not be considered to have breached any restriction on disclosure of information.

2.5. Anonymity

According to the Directive's preamble 34, it is up to each Member State to decide whether it should be possible to report anonymously or not and, in this connection, whether each Member State is obliged to follow up on anonymous reports.

If one or more Member States decide to only follow up on non-anonymous reports, it may cause doubt on whether employees (or external partners) at the end of the day are willing to report any breaches of EU law even though the employees (or external partners) will be protected from reprisals.

Notwithstanding, it is implied in the Directive's article 6(3) that persons who reported or publicly disclosed information on breaches anonymously, but who are subsequently identified and suffer retaliation, shall nonetheless qualify for the protection under the Directive.

In relation to anonymity, some member states have already implemented this term to its current whistleblower and it is expected that similar principle will be implemented in relation to the implementation of the new WB Directive. Either way, Vault Platform will also be able to ensure complete anonymity for all users of the platform, if they so choose, see section 3.2 below.

03

Information Requirements

3.1. The requirements

As stated above, the WB Directive sets up a number of requirements and/or recommendations related to the information which a reporting person must or should receive in relation to the person making the report.

It is recommended to ensure that a reporting person receives information which help the person to clarify/assess *whether the reporting will result in a protection under the WB Directive or not.* E.g. that the information is true, because if reporting person knows that if the information available to them at the time of reporting are not true, the person will not be protected under the WB Directive.

The WB Directive entails several requirements related to the possible information which should or could be provided to the reporting person:

- *Art 4(1) + (2):* Only information which has been reported in a **work-related context** is e.g. covered by the WB Directive, i.e. if the reporting person has obtained the information in any other context it will not be covered. However, the protection applies both where officials and other servants of the Union report breaches that occur in a work-related context inside and outside their employment relationship with the Union institutions, bodies, offices or agencies. The WB Directive shall apply to reporting persons working in the private or public sector who acquired information on breaches in a work-related context or work-based relationship. It is recommended that the User is informed about this requirement when commencing the reporting.

- *Art 6(1) a ((Premise (32)):* To enjoy protection under the WB Directive, reporting persons should have **reasonable grounds to believe,** in light of the circumstances and the information available to them at the time of reporting, that **the matters reported by them are true.** That requirement is an essential safeguard against malicious and frivolous or abusive reports as it ensures that those who, at the time of the reporting, deliberately and knowingly reported wrong or misleading information do not enjoy protection. At the same time, the requirement ensures that protection is not lost where the reporting person reported inaccurate information on breaches by honest mistake. Similarly, reporting persons should be entitled to protection under the WB Directive if they have reasonable grounds to believe that the information reported falls within its scope. The correct legal assessment of eligibility of the reporting persons in reporting should be irrelevant in deciding whether they should receive protection if the reporting persons motives are right.

Thus, the system should inform the reporting person that they must have *"reasonable grounds to believe that the information on breaches reported was true at the time of reporting and that such information fell within the scope of this Directive"* – including those additional areas that might be included through local implementation.

- *Article 6(3), 18 and 19 ((premise 93)):* **Retaliation** is likely to be presented as relating to grounds other than the reporting and it can be very difficult for reporting persons to prove the link between the reporting and the retaliation, whilst the perpetrators of retaliation may have greater power and resources

to document the action taken and the reasoning. Therefore, **once the reporting person demonstrates prima facie that he or she reported breaches** or made a public disclosure in accordance with this Directive and suffered a detriment, the **burden of proof should shift** to the person who took the detrimental action, who should then be required to demonstrate that the action taken was not linked in any way to the reporting or the public disclosure.

On this basis, it is recommended that the system's acknowledgement of receipt provide adequate details about the reporting allowing the reporter to demonstrate that the reporting was made in accordance with the Directive.

3.2. How are these requirements met with Vault Platform?

In order to ascertain whether the incident in question constitutes a breach of Union law and/or whether the reporting person will be protected by the WB Directive, the whistleblowing mechanism must enable trusted and secure two-way communication between the whistleblower and employer/company. This may also require that the identity of the reporter remains anonymous throughout the process.

Vault Platform is designed as a trusted incident reporting and resolution solution where employees would feel safe to raise concerns with their employer directly. The aim is for employee and employer to reach a resolution before the employee feels the need to take their concerns to an external party.

Through the Vault App, a potential whistleblower is able to report a concern and start a dialogue with a relevant stakeholder at the employer. The reporter may identify themselves or remain anonymous and ask and respond to questions from their appointed case manager. The Vault App also serves as a method of showcasing relevant information such as policy documentation or training assets (specific for the employer/company), through which it can inform the reporter about the protections and stipulations of the Directive.

By securely restricting involvement in the process to the relevant parties (i.e. the incident reporter and their appointed case manager) and eliminating other persons such as the reporter's line manager, Vault Platform reduces incidents of retaliation. In the event that retaliation does take place, Vault Platform can be used to report and resolve on that as well.

04

Personal Scope - Access Requirements Directive

4.1. The requirements

The Directive provides that the protection against retaliation is granted both to persons who report information on acts or omissions within an organisation (“internal reporting") or to an external authority (“external reporting") and to persons who make such information publicly available. Reference is made to clause 2.4 above.

The WB Directive premise (55) stipulates that:

> "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'), but also, to any extent possible, by any of the group's agents and suppliers and by any persons who acquire information through their work-related activities with the entity and the group."

Effective enforcement of Union law requires that protection should be granted to the broadest possible range of categories of persons, who, irrespective of whether they are Union citizens or third-country nationals, by virtue of their work-related activities, irrespective of the nature of those activities and of whether they are paid or not, have privileged access to information on breaches that it would be in the public interest to report and who may suffer retaliation if they report them. Member States should ensure that the need for protection is determined by reference to all the relevant circumstances and not merely by reference to the nature of the relationship, to cover the whole range of persons connected in a broad sense to the organisation where the breach has occurred.

- Article 4(2) + (3): The system must (also) provide access for employees whose position has been terminated or not begun yet.

- Article 4(4) + Article 8(2): The system must (also) provide access for (a) facilitators; (b) third persons who are connected with the reporting persons and who could suffer retaliation in a work-related context, such as colleagues or relatives of the reporting persons; and (c) legal entities that the reporting persons own, work for or are otherwise connected with in a work-related context.

Article 8, however, solely states that the internal channel *"may enable other persons, referred to in points (b), (c) and (d) of Article 4(1) and Article 4(2), who are in contact with the entity in the context of their work-related activities to also report information on breaches."*

- Article 9(2) – ((Premise 53)): The system should upon request by the reporting person offer that there is also a possibility to enable reporting by means of physical meetings, within a reasonable timeframe.

- Article 18(4): Where a person requests a meeting with the staff members of legal entities in the private and public sector or of competent authorities for reporting purposes pursuant to Articles 9(2) and 12(2), legal entities in the private and public sector and competent authorities shall ensure, subject to the consent of the reporting person, that complete and accurate records of the meeting are kept in a durable and retrievable form.

- Article 18(2) + (4): The systems should grant access for the reporting person to offer *"the opportunity to check, rectify and agree the minutes of the meeting by signing them."*

- Article 22(1): The system should ensure that that persons concerned fully enjoy the right to an effective remedy and to a fair trial, as well as the presumption of innocence and the rights of defence, including the right to be heard and the right to access their file.

To sum up the protection provided in Articles 4 to 6 divide the persons protected in the following groups:

1. Reporting persons working in the private or public sector and who have acquired information about infringements in a work-related context,

2. Reporting persons, if they report or publish information acquired in an employment relationship, which has since ceased.

3. Reporting persons whose employment has not yet commenced in cases where information of an infringement has been acquired during the period of employment or other pre-contractual negotiations.

In addition to the reporting person, the protection also includes:

4. Mediators,

5. Third parties who are connected to the reporting person and who may be subjected to reprisals in a work-related context such as colleagues or relatives of the reporting person, and

6. Legal entities that the reporting person owns, works for or is otherwise associated with in a work-related context.

Article 21(6) states that persons referred to in Article 4 shall have access to remedial measures against retaliation as appropriate, including interim relief pending the resolution of legal proceedings, in accordance with national law.

4.2. How are these requirements met with Vault Platform?

Vault Platform's Open Reporting capability satisfies Article 4(4) and 8(2) by providing access to the same speak up solution for other members of the organisation's ecosystem that are not integrated with the corporate directory (i.e. new employees not yet onboarded, suppliers, customers, contractors and casual workers, even members of the public). The web-based reporting interface works on any device and enables people to submit reports that are automatically routed to the most appropriate internal stakeholder.

Vault Platform satisfies Article 4(2) and (3) for new employees not yet onboarded through Open Reporting (see above). For terminated employees or those leaving the organisation the Vault App can be configured to remain accessible for a defined period of time with all the same features and functionality.

Vault's Resolution Hub, the case management system, enables privileged access (by user invitation only) to third parties such as external mediators, lawyers or consultants, who are invited to take part in the investigation and / or resolution of the case.

With automated triage and routing, Vault Platform ensures new incident reports are flagged to the most appropriate stakeholder immediately and once a report is submitted opens up a secure channel of communication between the reporter and the case manager. This ensures that a follow up (including the arrangement of physical meetings) can be carried out within a reasonable timeframe.

As well as enabling real-time two-way communication between incident reporter and case manager, Vault Platform's Resolution Hub securely stores and time stamps all notes, minutes, evidence, data, and other information in one place. An audit log securely tracks each and every change made to a case.

The full report file can be exported as PDF at the push of a button and data can be exported into another system for archiving or further analysis.

05

Confidentiality/Non-Disclosure Requirements

In order to enable effective communication with staff members who are responsible for handling reports, it is necessary that the competent recipients for whistleblowing have in place channels that are user-friendly, secure, ensure confidentiality for receiving and handling information provided by the reporting person on breaches, and that enable the durable storage of information to allow for further investigations. This could require that such channels are separated from the general channels through which the competent recipients communicate with the public, such as normal public complaints systems or channels through which the competent authority communicates internally and with third parties in its ordinary course of business.

In terms of the system, it is necessary that staff members who are responsible for handling reports and staff members of the competent authority who have the right of access to the information provided by a reporting person comply with the duty of professional secrecy and confidentiality when transmitting the data both inside and outside the competent authority, including where a competent authority opens an investigation or an internal enquiry or engages in enforcement activities in connection with the report.

Safeguarding the confidentiality of the identity of the reporting person during the reporting process and investigations triggered by the report is an essential ex-ante measure to prevent retaliation. It should only be possible to disclose the identity of the reporting person where that is a necessary and proportionate obligation under Union or national law in the context of investigations by authorities or judicial proceedings, in particular to safeguard the rights of defence of persons concerned. The protection of confidentiality should, however, not apply where the reporting person has intentionally revealed his or her identity in the context of a public disclosure.

From the WB Directive, the confidentiality requirement is stipulated in varies ways:

- Article 9(1)(a): The system must be *"(…) designed, established and operated in a secure manner that ensures that the confidentiality of the identity of the reporting person and any third party mentioned in the report is protected, and prevents access thereto by non-authorised staff members;"*
- Article 16 (1) + (2): The system must *"ensure that the identity of the reporting person is not disclosed to anyone beyond the authorised staff members competent to receive or follow up on reports, without the explicit consent of that person".*
    - NB: The requirement is beyond a mere system requirement as described on article 9 as it also applies to the staff member handling the reporting.
- Article 6(3) ((Premise 93)): In case anonymity is compromised, the system must nevertheless still secure that the reporter can access enough details about the reporting to demonstrate that the reporting was made in accordance with the Directive
- The system must ensure that *"reporting persons are informed before their identity is disclosed, unless such information would jeopardise the related investigations or judicial proceedings".* Meaning that if the identity is disclosed, cf. above re. article 16 (1) + (2), does the reporting person then receives information about the disclosure?

5.1 How are these requirements met with Vault Platform?

Vault Platform is designed to nurture an environment of trust. Reporting persons are able to use the Vault Platform to submit incident reports and communicate with the investigating case manager while remaining anonymous if they so desire. Vault Platform ensures that Case Managers are able to respond to and proactively communicate with anonymous incident reporters through a secure chat system, and all data is encrypted both in-transit and at rest. Vault Platform complies with ISO27001 – the international standard for information security.

Furthermore, each user within the Vault Platform system is ringfenced. Incident reporters have no visibility of each other; Case Managers have no visibility of or access to reports other than those designated specifically to them; and while Administrators are able to observe Case Manager activity, they cannot involve themselves in a specific case without taking control of that case from the current Case Manager.

06

Progress Requirements

According to article 7(2), the Member States shall encourage reporting through internal reporting channels before reporting through external reporting channels, where the breach can be addressed effectively internally and where the reporting person considers that there is no risk of retaliation. Further, in Article 7(3), it is stated that appropriate information relating to the use of internal reporting channels referred to in paragraph 2 shall be provided in the context of the information given by legal entities in the private and public sector pursuant to point (g) of Article 9(1).

Various process requirement are stipulated in the WB Directive such as:

a) Article 9(1)(b): Does the person reporting receive an *"acknowledgment of receipt of the report to the reporting person within seven days of that receipt;"*

b) Article 9(1)(d): Does the system set up a *"Diligent follow-up by the designated person",* e.g. is there a proposed deadline for follow-up, cf. subsection (f)?

c) Article 9(1)(f) – ((Premise 58)): Does the system set up "a reasonable timeframe to provide feedback, not exceeding three months from the acknowledgment of receipt or, if no acknowledgement was sent to the reporting person, three months from the expiry of the seven-day period after the report was made"?

d) Article 9(1)(g): Does the system have "provision of clear and easily accessible information regarding the procedures for reporting externally to competent authorities pursuant to Article 10 and, where relevant, to institutions, bodies, offices or agencies of the Union."?

e) Article 17: "Any processing of personal data carried out pursuant to this Directive, including the exchange or transmission of personal data by the competent authorities, shall be carried out in accordance with Regulation (EU) 2016/679 and Directive (EU) 2016/680. Any exchange or transmission of information by Union institutions, bodies, offices or agencies shall be undertaken in accordance with Regulation (EU) 2018/1725. Personal data which are manifestly not relevant for the handling of a specific report shall not be collected or, if accidentally collected, shall be deleted without undue delay."

f) Article 18(1): Does the system ensure that "Reports are stored for no longer than it is necessary and proportionate in order to comply with the requirements imposed by this Directive, or other requirements imposed by Union or national law"?

g) Article 18(2): Does the system support reporting via phone?

h) Referring to Article 18(2) which states: 'Where a recorded telephone line or another recorded voice messaging system is used for reporting, subject to the consent of the reporting person, legal entities in the private and public sector and competent authorities shall have the right to document the oral reporting in one of the following ways: (a) by making a recording of the conversation in a durable and retrievable form; or (b) through a complete and accurate transcript of the conversation prepared by the staff members responsible for handling the report. Legal entities in the private and public sector and competent authorities shall offer the reporting person the opportunity to check, rectify and agree the transcript of the call by signing it.

According 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. The safeguards and requirements referred to in Article 9(1) shall also apply to entrusted third parties operating the reporting channel for a legal entity in the private sector, such as Vault Platform.

6.1. How are these requirements met with Vault Platform?

Vault Platform satisfies all requirements in Article 9(1) as per the information in section 4.2. Regarding Article 9(1)(g), the Vault App serves as an easily accessible place to store and showcase policy documentation, information, and training materials.

Because it does not rely on incident reporting via telephone/hotline/call centre, Vault Platform eliminates the involvement of a third party (hotlines are typically outsourced to third-party call centres) thereby decreasing the level of friction in the process and reducing the opportunity for human error by immediately creating a durable text record validated by the reporting person. Any subsequent changes are captured in the audit log.

Vault Platform is fully compliant with GDPR and is ISO 27001 certified, complying with a set of industry procedures and policies relating to information security management.

07

Legislative References

WB Directive article	Topic	Paper reference
Article 1	Purpose of the Directive	Clause 1
Article 2	Material Scope of the Directive	Clause 2.2
Article 3	Relationship with other Union acts and national provisions	N/A
Article 4	Personal scope	Clause 4
Article 5	Definitions	N/A
Article 6	Conditions for protection of reporting persons	Clause 2.4, 2.5, 3.1 and 5
Article 7	Reporting through internal reporting channels	Clause 6
Article 8	Obligation to establish internal reporting channels	Clause 4.1 and 6
Article 9	Procedures for internal reporting and follow-up	Clause 4.1, 5 and 6
Article 10 - 14	Conditions to external channels	N/A
Article 15	Public disclosures	N/A
Article 16	Duty of confidentiality	Clause 5
Article 17	Processing of personal data	Clause 6
Article 18	Record keeping of the reports	Clause 4.1 + 6
Article 19	Prohibition of retaliation	Clause 2.4 and 2.5
Article 20	Measures of support	N/A
Article 21	Measures for protection against retaliation	Clause 2.4 and 4.1
Article 22 - 25	Measures for the protection of persons concerned, penalties, no waiver of rights and remedies and More favourable treatment and non-regression clause	N/A
Article 26	Transposition and transitional period	Clause 1
Article 27 - 29	Reporting, evaluation and review, entry into force and addressees	N/A

08

Status of and Effect of Implementation

Bird & Bird Law firm has developed an implementation tracker and a degree of change tracker for the EU Whistleblower Directive which contains information about the approach to implementation by EU Member States and a description of how significantly the implementation of the Whistleblowing Directive will change the existing laws.

Please find the trackers here:

Implementation tracker:

https://www.twobirds.com/en/in-focus/the-eu-whistleblowing-Directive/implementation-status

Degree of change tracker:

https://www.twobirds.com/en/in-focus/the-eu-whistleblowing-Directive/degree-of-change

vaultplatform.com

Bird & Bird

twobirds.com