III. WHISTLEBLOWER RULES AND REGULATIONS: THEIR RELEVANCE

City | Legal

What is a whistleblowing procedure?

- Provides a safe channel for “whistleblowers” that become aware of and wish to report breaches of law in various ways
- Frances Haughen, Julian Assange, Edward Snowden…

What is retaliation?

The principle: a whistleblower may not be subjected to ‘detrimental action’ on account of having made a protected disclosure…

“DETRIMENTAL ACTION…”

“OCCUPATIONAL DETRIMENT…”

The relevance of whistleblowing procedures

- Whistleblowers are typically **employees**, but can also be other third parties (i.e. service providers, contractors, shareholders)
- Statistically, whistleblowers are one of the main reasons behind increase in number of internal investigations being carried out in Europe today

Background (EU)

- Proposal for a European directive on whistleblowing had been under construction since 2016
- Twofold objective:
    1. Impose that every Member State has put in place whistleblower protection;
    2. Encourage harmonisation of whistleblower protection, and, consequently, the ‘modus operandi’ of investigations
- The EU Whistleblowing Directive was adopted in October 2019 and published in the Official Journal in November 2019

Background (Malta)

- Protection of the Whistleblower Act (Cap. 527) – 2013
- Amended in December 2021 to comply with the Directive
- Prior to the amendments, law applied only to government ministries and large companies with a minimum of 250 employees or very high threshold balance sheets / turnovers
- Today, all entities with >50 employees fall within its scope
- Where justified via risk assessment, entities with <50 employees may also be required to comply

Types of Disclosures

Internal Disclosures

External Disclosures

Public Disclosures

Anonymous Disclosures

Mandatory painpoints for employers

What matters are most relevant to investigations?

- Being aware of “improper practices” (reportable misconduct)
- Constructing an adequate reporting channel
- Confidentiality
- Data Protection
- Drawing up adequate policies

Reportable (alleged) misconduct

The list has been significantly widened. Some examples:

- A person **has failed, is failing or is likely to fail** to comply with any legal obligation;
- The health and safety of an individual has been, is being or is likely to be endangered;
- The environment has been, is being, or is likely to be damaged;
- A corrupt practice has occurred, is likely to occur or has occurred;
- A criminal offence has been committed, is being committed or is likely to be committed;
- A miscarriage of justice has occurred, is occurring or is likely to occur;
- Bribery has occurred, or is likely to occur or to have occurred;
- A person has failed, is failing or is likely to fail to comply with any legal obligation on consumer protection;
- A person has failed, is failing or is likely to fail to comply with any legal obligation on protection of privacy and personal data

and others! (Refer to the definition of “improper practice” in the Act).

Constructing an adequate reporting channel (1)

- Every employer shall have in place internal procedures for receiving and dealing with information about improper practices committed within or by that organisation
- The law regulates what the procedure should involve as a minimum…

Constructing an adequate reporting channel (2)

- A. Channels for receiving reports in writing OR orally, OR both. Oral reporting shall be made possible by telephone, other voice messaging systems, and, upon request, by means of a physical meeting
- B. Such channels to be operated in a secure manner that ensures the confidentiality of the identity of the whistleblower AND any third party mentioned in the disclosure
- C. Only authorised staff members should have access to this information (consider creating a dedicated committee that may then liaise with investigator(s) / disciplinary committee, human resources permitting)
- D. A WRO must be appointed, who shall receive the protected disclosure and maintain contact with the whistleblower

Constructing an adequate reporting channel (3)

- E. The WRO may and should request further information from the whistleblower if necessary
- F. The WRO is to acknowledge receipt of the internal disclosure within 7 days
- G. Feedback is to be provided to the whistleblower within 3 months
- H. In the event that disclosure leads to detection of a crime / contravention, the WRO may refer the report to the police

Constructing an adequate reporting channel (4)

- I. Disclosures are not to be made to heads / deputy heads of the organisation unless: (a) the organisation has no internal procedures in place; OR (b) the whistleblower believes that the WRO himself may be involved; OR (c) the whistleblower believes that the WRO is, by reason of conflict of interest, not a person to whom it is appropriate to make the disclosure
- J. Any channels must be GDPR-compliant by design

Confidentiality

Employers should operate their reporting channels in a secure manner and keep confidential the identities of:

"Whistleblower"
"Facilitators"
"Persons Concerned"

Data Protection

Any processing of personal data carried out pursuant to the Act shall be carried out in accordance with the General Data Protection Regulation (EU) 2016/679 (the "**GDPR**")…

(Purpose Limitation) 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…

Maintain **records** of all reports for as long as is necessary…

Records (1)

Where a recorded telephone line or another voice messaging system is used for disclosing (subject to the **consent** of the whistleblower), the WRO shall have the right to document the oral report by:

(i) Making a recording of the conversation in a durable / retrievable form; or

(ii) Through a complete and accurate transcript prepared by authorised staff members

Records (2)

Where an unrecorded telephone line or another unrecorded voice system is used for disclosing, the WRO shall have the right to document the oral disclosure in the form of accurate minutes of the conversation written by authorised staff members

Drawing up adequate policies

The employer is required to provide employees with “clear and accessible information about the existence of the internal procedures, and adequate information on how to use the procedures shall be published widely within the organisation and shall be republished at regular intervals.”

Why is it good to have robust whistleblowing policies?

- Good business and risk management
- Deters malpractice and avoids wrongdoing
- Protects staff, customers and the public
- Meets regulators’ expectations
- Encourages employees to raise matters internally, rather than externally
- Reduces financial loss

What about grievances / complaints that do not relate to improper practices?

- Upon receipt of a grievance / complaint, the employer should conduct an in-depth assessment to identify the suitable channel
- Care should be taken to direct the matter through the correct channel and involve the right people

IV. DATA PROTECTION CONSIDERATIONS

The applicable law

Regulation (EU) 2016/679, the GDPR – 25 May 2018

The Data Protection Act (Cap. 586)

Scope

The GDPR applies to:

- entities that are established in the EU, regardless of whether the personal data they process is of EU data subjects or not)
- Non-EU entities where the processing of personal data is in the context of offering goods / services to data subjects in the EU or the monitoring of behaviour of data subjects in the EU

The relevance of data protection

The GDPR should not be a barrier to carrying out the required internal investigations, but extra care must be taken to ensure compliance…

1) Data collections and reviews will nearly always involve the processing of personal data…

2) !! Failure to comply / demonstrate compliance could lead to claims for damages as well as hefty fines !!

Before the event

1. Be “GDPR-Ready”…

2. Establish the legal basis... (Art. 6(2) GDPR)

3. Provide employees with a privacy notice that explains, amongst other things, the legal basis on which you may be processing their personal data, the purposes for which their personal data may be processed and the rights they have…

4. Provide employees with details of how, if data is processed on the basis of legitimate interests, they can obtain more information on the balancing tests conducted…

Legitimate interest(s)

- **Legitimate interest(s)**
- **The “Legitimate Interests Assessment” (LIA)**
- **Can’t we rely on employee consent?**
- **Legal obligation?**

After the event (1)

1. If relying on legitimate interests, ensure you:

a. **Conduct a LIA and document it;**

b. **Have informed your data subjects of their right to object**

After the event (2)

2. (Purpose Limitation) Only use individuals' data in ways which they could reasonably expect, unless you have a compelling reason

3. Do not use individuals' data in ways they could find intrusive or harmful, unless you have a compelling reason

4. Implement safeguards to reduce impact where possible, such as restrictions regarding who can access the data and with whom it may be shared, as well as security measures to protect against unauthorised access

After the event (3)

5. If your LIA has identified a serious privacy impact, consider carrying out a Data Protection Impact Assessment (DPIA)

6. If the investigation involves the processing of special categories of data, further conditions of processing must be met

7. Continuing assessment and accountability

Monitoring employees – proceed with caution (1)

The investigation of employees can happen in different ways…

Whilst courts have made it quite clear that monitoring cases will be decided on the basis of the specific circumstances at hand, it is essential that some fundamental principles are observed…

Monitoring employees – proceed with caution (2)

Bărbulescu case

Subject? Monitoring of communication 'just because'

In 2016, the ECtHR ruled that employers violate employees' right to respect for private life if they secretly monitor employees' private communication without implementing **appropriate safeguards** to preserve employees' legitimate interests…

Monitoring employees – proceed with caution (3)

Bărbulescu case – continued

SIX PRINCIPLES FOR EMPLOYEE MONITORING WERE ESTABLISHED:

- the prior notification to employees of the possibility and the implementation of such measures and the disclosure of information regarding their exact nature;
- the extent of the monitoring, meaning the degree of limitations in time and space as well as the number of people with access to the footage;
- the legitimate reason to justify the monitoring;
- the possibility of implementing less intrusive methods;
- the severity of consequences of the monitoring; and
- the provision of legal safeguards for the employees.

Monitoring employees – proceed with caution (4)

Ribalda case

<u>Subject? Suspected theft</u>

In 2019, the ECtHR ruled that covert video surveillance of employees does not violate employees' right to respect for private life – *and the knowledge gained by the employer could be used as a justification for dismissal.*

Arguably 'watered down' the principles established in the **Bărbulescu case**.

Monitoring employees – proceed with caution (5)

Ribalda case – continued

The case regarded suspected theft in a supermarket over period of several months (8K-25K per month disappeared). Employer used covert CCTV to identify the guilty cashiers / sales assistants, who were then fired. The Grand Chamber decided that while covert monitoring is not justified for every slightest suspicion of wrongdoing, the surveillance in this case was justified.

Monitoring employees – proceed with caution (6)

Ribalda case – continued

The ECtHR:

- Weighed the protection of the privacy of employees against the employer's property and business operations, considering that there was a legitimate aim due to the employer having had a reasonable suspicion of a serious misconduct causing the company substantial losses
- Considered that the expectation of privacy on the part of employees was limited as they were being monitored in a place that could not be deemed 'private'
- Duration of surveillance had not exceeded that which was necessary to confirm suspicions
- Footage had only been viewed by certain select individuals
- Surveillance had not been used for any purposes other than to investigate the thefts and to take the disciplinary measures against those responsible

Monitoring employees – proceed with caution (7)

Key takeaway? Whereas Bărbulescu related to an employee 'merely' using a messaging application to send private messages whilst at work, Ribalda concerned the use of covert CCTV to uncover criminal activity in the workplace.

In light of all of the above considerations, possible approaches include: (i) limiting the timeframe of your review; (ii) limiting those who access the data; (iii) using focused search terms / technology assisted review to restrict what is being reviewed; (iv) ensuring there is a justifiable reason behind what you are doing; (v) ensuring that your DPO is consulted and kept informed; and (vi) ensuring that all policies and procedures internally are adequate and bring all necessary information about employee monitoring to employees.

Further points of note regarding monitoring

Where possible:

- **Inform employees** that they are being monitored before the fact
- **Do not monitor or review private information.** Remember: does the employee expect a degree of privacy? Difficult to justify breaches of privacy in the context of private devices (BYOD), for example

Data Protection and Whistleblowing Programmes

a. LEGAL BASIS
b. SPECIAL CATEGORIES OF DATA
c. DATA PROTECTION IMPACT ASSESSMENT
d. NOTICE
e. DATA SECURITY (TECHNICAL AND ORGANISATIONAL MEASURES)
f. PROCESSORS
g. DATA BREACHES
h. TRAINING

WP29 Opinion

- In 2006, Article 29 Working Party (now the European Data Protection Board (EDPB)) issued an Opinion on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime (the "**WP29 Opinion**")

- Although the WP29 Opinion pre-dates the GDPR, many of the recommendations will likely remain relevant until the EDPB issues superseding guidance:

  e.g. that personal data processed in the context of a whistleblower report should be deleted, promptly and usually within two months of completion of the investigation of the reported allegations. These periods may be extended if legal proceedings or disciplinary measures are initiated.

Data Retention

- The GDPR does not provide specific data retention periods
- Data should not be held for longer than is needed and shouldn't be kept “just in case”
- Establish clear data retention policies and document them
- Always attribute your decision to keep a specific data-set to a lawful basis

THANK YOU

Dr Emma Grech
emma.grech@thecitylegal.com

City | Legal