Practical Implications (B)

DATA PROTECTION

City | Legal

www.21Academy.education

The applicable law

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

The Data Protection Act (Cap. 586)

City | Legal

www.21Academy.education

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…

(Storage Limitation) Maintain **records** of all reports for as long as is necessary…

City | Legal

www.21Academy.education

Confidentiality

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

- “Whistleblower”
- “Facilitators”
- “Persons Concerned”

City Legal

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

City Legal

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

City | Legal

www.21Academy.education

Improper Practice

"a person has failed, is failing or is likely to fail to comply with any legal obligation on the protection of privacy and personal data, and the security of network and information systems to which he is subject"

Data Protection Considerations (1)

Ensuring your whistleblower channel is GDPR-compliant

- Legal Basis
  - Legal obligation vs legitimate interests
  - Special categories of data
- Purpose Limitation
- Data Minimisation
- Storage Limitation
  - "… reports shall be stored for no longer than is necessary and proportionate in order to comply with the requirements imposed by this Act …"
- Confidentiality
- Third party partners
  - Processors
- Accountability – periodic reviews
- Involve your DPO

City | Legal

Data Protection Considerations (2)

Right to information

- The employer has the obligation to inform all whistleblowers about the processing activities in connection with the reporting and the subsequent investigation process and about the protection of their data in accordance with Article 13 GDPR. Preferably this information should be included in the whistleblowing channel.
- However, the right to information and the effectiveness of the investigation of breaches may be seen to be ‘at odds’, particularly as the personal data contained in the report may relate to third parties (including the accused!). In such cases, a documented decision to postpone providing the accused with certain information may be necessary.

City | Legal

Data Protection Considerations (3)

Data Subject Access Request (DSAR)

- What is a DSAR?
- The DSAR may also seem to be ‘at odds’ with the whistleblowing investigation.
- The European Data Protection Board (EDPB) advises that if access is granted to a concerned individual, all the personal data of the whistleblower and any third parties should be redacted from the documents concerned. Where this is not practicable, it may be possible to withhold the disclosure of an individual’s personal data on the basis that this would interfere with the rights and freedoms of another individual.

City | Legal

Data Protection Considerations (4)

Data Retention (Storage Limitation)

- 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

City Legal

Data Protection Considerations (5)

Data Retention (Storage Limitation) (Continued)

- In 2006, Article 29 Working Party (now the 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.

City | Legal

Data Protection Considerations (6)

Privacy by design/default

- Employers are required to take all reasonable technical and organisational precautions to preserve the security of personal data that is gathered in the context of a whistleblower report
- The aim is to protect that data from accidental or unlawful destruction or accidental loss and unauthorised disclosure or access
- It is important to put in place appropriate security measures in order to prevent personal data from being accessed by non-authorised persons

City | Legal

Conclusion

City | Legal

Know your obligations

The law became effective immediately.

Step 1: Figure out if you are required to have an internal reporting channel in place

Step 2: If so, ensure that you identify the right people in order to set up your 'whistleblowing team'

Step 3: Ensure your organisation is trained in the new law

Step 4: Set up your whistleblowing channel

Step 5: Create your policies…

Step 6: Keep abreast of developments!

City | Legal

THANK YOU

Dr Emma Grech
emma.grech@thecitylegal.com

City | Legal