Intelligence sharing for enforcement
Data protection & privacy

16/04/2015
Contents

1. Intelligence sharing – who and what
2. Personal data protection
3. Trade secrets
4. Access to information implications
5. Information use in enforcement context
6. Conclusions
Intelligence sharing

Art 12: Competent Authorities shall

• cooperate with each other; administrative authorities of third countries; Commission to ensure compliance.

• exchange information on serious shortcomings detected through checks, and on the types of penalties imposed, with each other and the Commission
Who is sharing information

• Exchange between:
  • Competent authorities & related MS enforcement officials
  • Administrative authorities of third countries – producer and e.g. USA/Australia
  • European Commission
What information?

- ‘Nominal’

- Intelligence that does not have immediate relevance to a particular investigation – e.g. risks re particular countries/species/suppliers

- Intelligence that is relevant to a particular investigation with cross-jurisdiction application

- Details of ongoing/concluded investigations
Personal data protection

• Relevance:
  • name of a company director, supplier, complainant...

• ‘Processing’ of personal data is controlled

• Principles: lawfulness, purpose limitation, proportionality, accuracy, retention period

• Obligations on data controllers

• Data re offences / suspected offences / convictions

• Transfer between Member States / Commission / Outside EU
Personal data protection

Implications:

• Data controllers should be identified
• Data subjects should be informed (exceptions exist)
• Access to some data – ‘need to know’ basis
• Guidance on how to process data
• Transfer to third countries: USA; Australia.
  • Exception: where transfer is necessary to establish legal claims
• Model contract
Trade secret requirements

- E.g. commercial data on customers, suppliers, business plans.
- Protection against unlawful acquisition, use, disclosure.
- Use and exchange of information for investigation/enforcement activities is allowed.
- Need to protect against unauthorised acquisition/use → security of communication method.
Access to information

• For data subjects in context of personal information
  • Exception - if necessary to safeguard monitoring/regulatory function

• Access to information provisions
  • Exceptions – proceedings of public authorities, commercial confidentiality, personal data, interests of the person who supplied the information

• Potential for ‘forum shopping’
Using intelligence in enforcement

• Use of intelligence in a prosecution if collected by authorities in a different jurisdiction can = complex

• Timing: when is information shared / different parties (e.g. CAs in different Member States) involved.

• Role of multilateral organisations to support?
Summary conclusions

- Legal considerations are applicable to different types of information

- Legal considerations/requirements:
  - Exist – personal data protection and secure and appropriate communication are key
  - Are manageable
  - Are present whether or not an intelligence sharing ‘mechanism’ is used
  - A ‘mechanism’ = one option to ensure they are dealt with properly
Thank you

Emily Unwin
eunwin@clientearth.org

www.clientearth.org
@ClientEarth