



International Investigations: Issues to Consider When Conducting or Defending Against an FCPA Investigation Outside the United States

Presentation to:

Ninth Annual Pharmaceutical Regulatory and Compliance Congress
Washington, DC
October 27-29, 2008

Presented by: Sandee I. Priser
Ernst & Young LLP
Chicago, IL

Leslie A. Shubert, Esq
Sidley Austin LLP
Washington, DC

Issues for Consideration

- Privacy Issues
- Maintaining Privilege
- Subpoenas and Discovery Requests for Information Outside the U.S.
- Interviewing Witnesses Abroad
- Taking Advantage of Foreign Laws

Privacy Issues

- EU Data Protection Directive
- Accessing Employee Information
- EU Data Maintenance Requirements
- Disclosure to Third Parties
- Data Transfers from the EEA
- Country-Specific Examples
 - Belgium
 - Switzerland
 - Non-EU Countries

EU Data Protection Directive

- EU Data Protection Directive 95/46/EC implemented by all EU Member States through national law often inconsistently
- Directive imposes obligations on data controllers in the EU as to how personal data may be processed and grants certain rights to data subjects
- Obligations during investigations may include:
 - Notice to national Data Protection Authorities
 - Notice to/Consent of Employees, Customers, Works Council
 - Limits to employee monitoring
 - Restrictions on disclosure and transfer outside EU
 - Preservation of data for disclosure in litigation
- Art 2: “‘Personal data’ shall mean any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”

Main obligations under the EU Data Protection Directive

- Personal data must be processed fairly and lawfully in line with purposes notified to the data subject and having satisfied at least one pre-condition for processing – e.g. consent or legitimate interest
- Sensitive personal data, including health data, may only be processed where more limited pre-conditions are satisfied the most common of which is having the explicit consent of the data subject
- Data controllers must ensure the personal data are adequate, relevant and not excessive for the purposes for which they are collected
- Data controllers must keep personal data accurate, up to date and for no longer than necessary
- Data controllers are responsible for ensuring appropriate technical and organisational measures are in place to protect the personal data and have written agreements in place with data processors processing the data on behalf of the data controller under which the processor ensures the same level of security
- Data controllers may not transfer personal data to countries outside the EU unless there is an adequate level of protection. Adequacy can be achieved in a number of different ways, consent, model contracts, safe harbour and binding corporate rules

Accessing Employee Information in the EU: Registrations, Notices and Works Council

- Registration with national Data Protection Authority may be required in some EU Member States
 - Statement of processing purpose and recipients
 - Check notice has been given as required by the employer and covers:
 - purpose of the investigation
 - recipients during the investigation
- Notice to Employees on Data Protection
 - Required in most Member States with limited exceptions
 - Data protection notice can be combined with document retention notice
- Works Council
 - Need to be informed or consulted
 - Depends on national law, Works Council rules and local practice
 - Existing approved policies permitting review of employee emails and documents
 - Consider when and how to inform/consult
- Consult local counsel for specific national requirements as requirements may vary in different Member States

Accessing Employee Information in the EU: Legitimate Processing and Monitoring

- Criteria for legitimate processing
 - Consent “informed and freely given”
 - “Explicit consent” required for sensitive data
 - Performance of contract
 - Legitimate interests
- Monitoring employees
 - Cultural and historical sensitivities vary throughout EU
 - Greece: may be prohibited even with consent, except where justified by requirements of security and safety in the workplace or judicial order
 - UK Employment Practices Code:
 - usually must make workers aware of monitoring and reasons for monitoring
 - monitoring systems subject to right of access by data subject, fair processing and other data protection requirements
 - monitoring of emails may be considered an interception and prohibited under telecommunications laws, e.g. in the UK under the Regulation of Investigatory Powers Act

EU Data Maintenance Requirements

- The duty to retain documents/data within the EU depends greatly on the EU Member State in which the documents are held and on the relevant regulatory bodies.
- For data protection, personal data should be held for no longer than is necessary. However, this needs to be balanced with legal and regulatory document retention requirements.
- For litigation purposes it is usually prudent to send a form of hold notice to relevant employees once that duty has arisen. Advice should be sought from local counsel for any data protection issues.
- The duty to retain documents for the purpose of litigation is often ongoing. Documents created during the course of an investigation must often be retained and are often disclosable in litigation.
- Consideration should therefore be given as to what documents are created during the course of an investigation and to whether they are protected by privilege.

Disclosure to Third Parties

- Disclosure of personal data to third parties is restricted by the EU Data Protection Directive
- Processing of personal data by third parties acting as data processors, e.g. audit firms, must be under a written agreement which includes obligations on the data processor:
 - To act only in accordance with instructions from the data controller
 - To implement appropriate and sufficient security measures
- Additional rules on transfers outside the EEA

Data Transfers from the EEA

- The EU's Data Protection Directive prohibits transfers of personal data to countries not considered to have adequate data protection laws, e.g., the U.S., unless certain exemptions apply
- Exemptions to data transfer restrictions include:
 - Consent
 - Model contracts
 - Binding corporate rules
 - U.S. Safe Harbor
 - Possibly where the transfer is necessary in legal proceedings, obtaining legal advice, or exercising legal rights

Country-Specific Examples

- Belgium
- Switzerland
- Brazil

Maintaining Privilege in an International Investigation

- Is attorney-client privilege recognized, and if so, what are its limits?
- Is attorney work product privilege recognized, and if so, what are its limits?
- In-house vs. outside counsel
- What steps are necessary to protect the privilege?
- How to protect, if privileged documents are seized by foreign government authorities or inadvertently produced?

EU Privilege Considerations

- Privilege for local jurisdictions vary markedly from within the EU and must be considered on a jurisdiction by jurisdiction basis.
- For EU commission investigations *Akzo Nobel Chemicals and Akcros Chemicals v Commission* (2007) applies.
 - No privilege for communications between in-house counsel and their business clients.
 - Preparatory documents, not exchanged with external counsel only protected if created exclusively for the purpose of seeking legal advice from external counsel in the exercise of rights of defence.
- Practical steps to assist protection of documents produced for internal compliance procedures in the context of Commission investigations:
 - Outside counsel must be instructed if privilege is to be created
 - State clearly on the face of each document that advice from external counsel is sought
 - Documents and memoranda produced should be addressed and sent directly to external counsel

Subpoenas and Discovery Requests for Information Outside the U.S.

- Subpoenas or document requests seeking documents from foreign affiliates of U.S. companies
 - Control
 - Conflict with foreign laws
- Use of Hague Convention
 - Letters of Request
 - Diplomatic or Consular Agents
 - Court-Appointed Commissioners

Interviewing Witnesses Abroad

- Check local law regarding restrictions on interviewing witnesses
- Issues regarding whether information obtained in witness interviews can be provided to regulators, e.g., SEC in the U.S. or to government agencies in other jurisdictions
- Examples
 - Swiss Penal Code, Article 271(1)

Taking Advantage of Foreign Laws in Defending Against Discovery, Government Investigations

- Representing witnesses in depositions who are under investigation or subject to potential prosecution outside the U.S.
- Representing foreign companies or their employees in interviews/depositions outside the U.S. by the U.S. government pursuant to letters rogatory or MLAT requests.

Practical Considerations for Investigation Teams

- Data acquisition
 - Careful planning required
 - Retention notification
 - Custodian list
 - IT considerations
 - Geography of custodians
 - Privacy rules
 - Non-US data stored in the US
 - Consent
 - Availability potentially limited due to local investigations

Practical Considerations for Investigation Teams

- Information processing and review
 - Data types
 - Accounting records
 - User files
 - E-mails
 - Processing/review locations
 - Country privacy laws in addition to EU laws
- Physical records
 - Collections and custodians
 - Off-site storage
 - Local technology limitations

Practical Considerations for Investigation Teams

- Investigation documentation
 - Balancing privacy with government reporting needs
 - Limited ability to transfer some information to the US
 - Protection from seizure by local prosecutors
 - Local management interest in reporting
 - Required notification to individuals in certain countries
- Interviews
 - Local language/cultural considerations
 - Required notifications in certain countries
 - Interview documentation