GLOBAL TRANSPARENCY REPORTING CONGRESS

8-9 April 2014

Effective Means of Supervising Data Disputes and Monitoring Privacy

Pulina Whitaker, Partner

Data Protection Considerations

- How do businesses balance transparency reporting obligations with European data protection obligations?
- Is it personal data?
- The difficult issue of consent to disclosure of personal data
- Disclosure to recipients outside EU
- New Data Protection Regulation – key changes

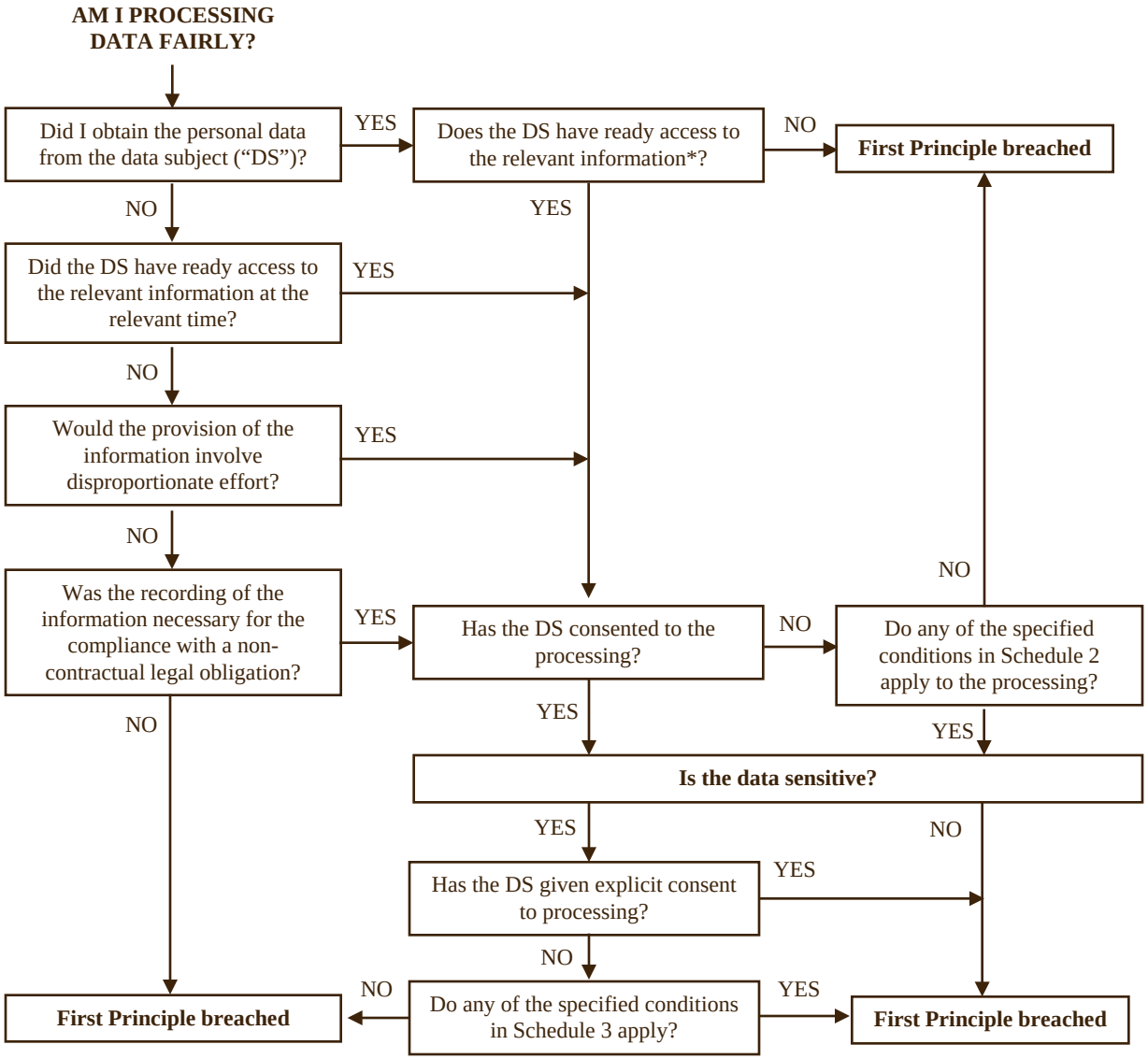
Balancing Reporting Obligations with Data Protection Obligations

- Different legal requirements and best practice guidelines on transparency reporting
- Global reporting considerations
- European data protection regime
- Striking a workable balance
- Informed consent from HCPs
- Make condition of the spend the disclosure of details and personal data
- Make condition of the spend the transfer of personal data

Consent

- Consent required to “process” personal data – unless exemption applies
- Explicit consent required to process “sensitive” personal data (race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, family life)
- Exemption to consent requirement:
  - necessary to perform a contractual obligation
  - to fulfil instructions from individual to enter into a contract
  - to comply with a non-contractual legal obligation
  - to protect the vital interests of the individual
  - necessary for the organisation’s legitimate interests
  - public interest
- Interpretation of consent varies throughout Europe
  - France – consent should be express/“opt-in”
  - UK – consent can be inferred; “opt-out” approach possible
  - European-targeted businesses should comply with most stringent standard

Consent


AM I PROCESSING DATA FAIRLY?
Did I obtain the personal data from the data subject ("DS")?
YES
Does the DS have ready access to the relevant information*?
NO
First Principle breached
NO
YES
Did the DS have ready access to the relevant information at the relevant time?
YES
NO
Would the provision of the information involve disproportionate effort?
YES
NO
Was the recording of the information necessary for the compliance with a non-contractual legal obligation?
YES
Has the DS consented to the processing?
NO
Do any of the specified conditions in Schedule 2 apply to the processing?
NO
YES
YES
Is the data sensitive?
NO
YES
Has the DS given explicit consent to processing?
YES
NO
NO
First Principle breached
Do any of the specified conditions in Schedule 3 apply?
YES
First Principle breached

Practical Consent Steps

- Include express and detailed consent provisions in contracts:
  - types of data collected
  - reasons for processing
  - include retention periods for data
  - third party recipients
  - transfers outside jurisdiction
- Data protection policies can include similar information and include subject access procedure and right to have their data deleted
- Tell individuals they must notify of changes to personal data already provided

International Data Transfers

- Physical transfer or where data can be accessed from outside Europe over a computer network
- Transfers may only take place to a country providing an adequate level of protection unless statutory exception applies
- Countries providing “adequate level of protection”:
  - EEA countries
  - Argentina
  - Canada
  - Guernsey
  - Isle of Man
  - Jersey
  - Switzerland
  - Andorra
  - Israel
  - The Faroe Islands

International Data Transfers - Statutory Exceptions

- Transfers outside EEA also legitimate where:
  - to a Safe Harbor registered company in the US;
  - parties have signed “model contractual clauses” in EU approved form;
  - approved binding corporate rules in place in multinationals;
  - data subject expressly consented to transfer;
  - other exceptions:
    - necessary to perform a contractual obligation to the individual;
    - necessary for company’s compliance with a legal obligation;
    - necessary for company to establish or defend its legal rights; or
    - necessary for reasons of substantial public interest

New EU Data Protection Regulation - Key Changes

- Data subject definition:
  - identified person
  - identifiable person by likely methods including by reference to a number, location or online identifier or factors specific to e.g. physical, genetic, mental, economic, cultural or social identity
- Personal data definition:
  - “any information” relating to a data subject
  - not limited to identifying information
  - different interpretations in EU countries?
- Explicit consent required – controller must prove consent if challenged
- Consent may not be sufficient if imbalance of power between the business and the individual

New EU Data Protection Regime - Key Changes (cont'd)

- Controller must tell individuals about how data is processed, any appointed DPO, recipients of data, retention, right to contact DPA
- Transfers: new Binding Corporate Rules for processors
- Appoint Data Protection Officer – if business has 250+ employees or processing is a core function
- Data portability right
- Right to be forgotten
- Privacy by design/default

New EU Data Protection Regime - One-Stop Regulatory Shop

- Multi-nationals can deal with one regulatory authority (DPA)
- Choose DPA in main country of establishment or where main processing takes place (for non-EU businesses) – e.g. UK?
- No need to register with all European DPAs
- Non-exclusive authority of lead DPA
- Mutual assistance of all DPAs for cross-border issues

New EU Data Protection Regime - Data Protection Officer

- Requirement to appoint a Data Protection Officer – if a business has more than 250 employees or processing is core function
- Signifies top-level commitment to data protection issues
- Designated contact person for DPA
- Need for training and support
- Within legal function (to maintain legal privilege)
- Appointed for at least two years
- Communicate name of DPO to DPA and to relevant employees or customers
- Role:
  - advise business of its obligations
  - monitor policies
  - monitor compliance with Regulation
  - liaise with DPA as needed

New EU Data Protection Regime - Non-EU Businesses

- Businesses targeting EU consumers will need to comply
- Current application to non-EU businesses using EU equipment (e.g. servers) or processors
- Appoint an EU representative
- Transfers outside the EU:
  - explicit consent or assessment of adequacy
  - safe harbor (to the US)
  - necessary transfer
  - Model Clauses
  - Binding Corporate Rules - controllers
  - new Binding Corporate Rules - processors
  - Enforcement?

New EU Data Protection Regime - Penalties

- Most EU countries limit data protection breaches to around £500,000 per breach - average is £100,000 - FSA fines significantly more
- Higher penalties for breach of new Regulation
- Written warnings
- New fines up to 5% global turnover or €100,000,000
- Compulsory reporting of data security breaches - to DPA and individuals (if breach adversely affects privacy) - within 24 hours
- Individual rights to sue controllers and processors

Reporting strategies

- Which countries are affected
- Where are recipients of reports located
- What disclosure rules apply
- Get consent from HCPs to disclose and transfer personal data abroad
- Consult with internal compliance and legal teams
- Plan to deal with no consent / withdrawal of consent
- Document your processes

Personal Data Disputes with HCPs

- Consent:
  - challenge
  - withdrawal
- Accuracy of personal data
- Dispute regarding disclosure of data
- Privacy considerations

Proactively manage HCP Data Disputes

Pre-submission review:

- Consider voluntarily providing HCPs the opportunity to review the data prior to submission to the review authority
- Not mandated, but could be extremely useful in reducing HCP data disputes and improve customer relations
- Could also help improve accuracy of data submitted the government or other reviewing authority

Proactive Education Efforts

- Education of covered recipients
  - Notifications of payments or transfers of value
  - “Dear Doctor” letters

- Education and training of appropriate personnel
  - Field sales force
  - Other Personnel interacting with covered recipients
  - Personnel responsible for compiling data and preparing report

- Education of third parties
  - Vendors
  - Affiliated entities, including foreign affiliates and distributors

Monitoring and Auditing

- Continual monitoring of the reporting process and systems

- Periodic audits of payments and transfers of value: consider reviewing documentation (e.g., receipts, sign-in sheets, etc.) and source systems (e.g., Concur, SAP, etc.) underlying the payment to ensure that data on the company's report is in fact consistent with the company's documentation and systems