

## Navigating the International Data Protection Maze

**Peggy Eisenhauer**  
Privacy & Information  
Management Services



*session three*

Applying Data Protection Rules  
to Global Screening Programs





## Contextual Reality Check

- Before you do anything else, figure out what rules apply!
  - Are you screening a US worker for a US job?
  - ...screening a US worker for a foreign job?
  - ...screening foreign worker for a US job?
  - ...screening a foreign worker for a foreign job?



## What Laws to Apply

- National DP laws generally protect data about residents of the nation
- Data transfer restrictions in EU laws are designed to ensure that the DPA has authority, by limiting the ability of controllers in country to transfer data to other countries
- Other countries (such as the US and Canada) impose accountability on local controllers, regardless of where the data is processed
- Companies also have to comply with local laws



## What Laws to Apply

Worker Nationality	Job Location	Law(s) to Apply
US	US	US
US	Foreign	Foreign & US
Foreign	US	Foreign & US*
Foreign	Foreign	Foreign

\* Foreign laws will likely restrict access to data used for the screening process



## Cooperative Enforcement

- Many multi-national initiatives exist to enable cross-border enforcement
- APEC privacy framework is testing cross-border privacy rules (CBPRs), using government and NGO accountability agents
- The US FTC actively cooperates with foreign DPAs on enforcement matters



## Example: Accusearch, Inc.

- Accusearch is a US-based company that provides criminal background searches via the web
- Accusearch provided background searches on Canadian residents without providing notice or obtaining consent
- The Canadian Federal DPA concluded that these searches violated Canadian law
- At the request of the DPA, the US Federal Trade Commission filed an action against Accusearch and the US District Court permanently enjoined the activity
- The ruling was upheld by the 10<sup>th</sup> Circuit



## Know Your Role

- If you are screening in Europe or any country with DP laws, understand if the law establishes different rules for controllers and processors
- Controllers in the EU must register their data processing activities
- Controllers are accountable to DPAs and data subjects for inappropriate processing
- Processors cannot make decisions about the processing, but have fewer legal obligations and risks




## Processor vs. Controller

- In most cases, vendors are processors – you only screen workers at the direction of the controller
- If your client is established in the country, it should be familiar with local laws
- If your client is established in the region, you should verify that it is aware of local laws
- If your client is not familiar with local laws, you must be clear about how compliance obligations are allocated



## Understand the Challenges

- What laws exist in the target jurisdiction?
- What are the cultural norms in the target jurisdiction?
- What data is available? Is it available to the employer or only to the candidate?
- Do I have to obtain consent? If so, are there form or content requirements? Does the consent form need to be in a particular language?
- Are there other rules? Can I transfer the data to a client outside of the target country? If so, are there steps I need to take to authorize the transfer?



## Accept that You Can't Port Your US Compliance Process

- The FCRA and US state screening laws require very specific CRA processes –client certifications, notice and consent form language, report content limits – as well as specific steps to deal with adverse results
- Yet US laws permit broad searches (regardless of the job) – and US laws also permit open-ended consents that can be used both pre-employment and post-hiring
- US laws also permit rejection if the candidate doesn't consent



## Key International Differences

- Data that US-based entities obtain as a matter of public record (such as criminal records) is considered highly-sensitive in other countries
- Data that US-based entities obtain as a matter of course (such as credit data or personal references) is considered irrelevant in other countries
- Notices and consents must meet other applicable legal requirements for content and language




## Key International Differences

- In many countries, you can't run searches that aren't strictly related to the job – even if the candidate consents
- You can only require a candidate to consent if the search is truly necessary for the position and no other path exists to qualify the candidate
- Consent is limited to the particular search, at the particular moment, for the particular job
- Companies may have real liability for refusing to hire a candidate who refuses to consent to an overbroad screening



## Data Collection – General Requirements (UK Model)

- DP laws generally favor data collection from the individual directly
  - Data can be verified to establish truth
  - Data should be collected from 3<sup>rd</sup> parties only when there are “significant risks involved” and there is no less intrusive alternative
- Provide notice regarding the collection – clearly identify the employer and (if applicable) the recruitment agency
- Clearly indicate what information is required from the candidate and how it will be used – if you request optional information, indicate that it is not required



## Data Collection – General Requirements (UK)

- Only request information that is related to the job
  - For example, only request criminal conviction data if relevant for the position – and then only request information on offenses that would have a direct bearing on the person's suitability for the job
  - Only request sensitive information if strictly needed
- Only request information needed for the moment – collect consent for screening at the end of the process; collect info needed for payment upon hire
- Provide information on the nature and sources of 3<sup>rd</sup> party information that may be used



## Verification of Data – UK

- Inform candidates of the nature of planned verification and the methods – identify external verification sources
- Do not require candidates to use access rights to obtain verification information
- Verify criminal history disclosures using established and approved processes
- You must receive a signed consent from the candidate to secure the release of information from other organizations or agencies
  - Requesting information without a consent is a criminal offense



## Verification of Data – UK

- Employer and recruiting agency staff must be trained on handling of discrepancies found during the verification process
- The applicant must have an opportunity to respond to any discrepancies



## Pre-employment Vetting – UK

- Strong legal preference for verification over vetting
- “Only use vetting where there are particular and significant risks involved to the employer, clients, customers or others, and where there is no less intrusive and reasonably practical alternative”
- Do not vet candidates merely because customers request/require it – each company must independently determine that vetting is justified for a particular position
- Conduct vetting as late as possible in the process (e.g., as final condition to hire)



## Pre-employment Vetting – UK

- Notify candidates of the nature and source of vetting that will occur – notice should be made in the application materials – and obtain consent for the specific searches
- Only obtain vetting data from reliable, reputable sources
- Only gather specific information from vetting sources – you cannot screen to obtain general background information about the candidate



## Pre-employment Vetting – UK

- The searches conducted must be relevant for the job (e.g., driving check only if job involves driving, credit check only if the job involves financial transactions)
- Criminal history search results cannot include spent convictions (unless you have specific legal authorization)
- The search results must not reveal information about other persons (spouses, family members)
- The candidate must have an opportunity to respond to any adverse information in search results




## Media Checks

- Searching candidates in the media (newspaper archives) or online is generally not permitted in countries with data protection laws for either verification or vetting
- Sources are not considered reliable
- Sources may reveal inappropriate additional information
- In many countries, screening data may only be obtained from approved sources (such as the central registry)



## Records Management – UK

- Application data and vetting search results should only be retained in the employment file if it is clearly necessary for the on-going employment relationship
- For criminal records, only retain the fact that a check was conducted and whether the result was satisfactory or not
- Unsuccessful candidates must have the ability to have their entire record deleted
- All personal data must be appropriately secured (and securely destroyed)



## Records Management - Elsewhere

- Records retention is one of the most variable aspects of DP law
- EU law prohibits retention of personal data once the purpose for which it was collected has been fulfilled
- Other countries require retention in order to enable data subject to exercise access rights



## Notice and Consent Forms – General Requirements

- Clearly identify the data controller (the employer) and any other part that is involved in the data collection process
- Indicate what data is being requested, the purposes for the collection, how it will be used, with whom it will be shared, and how long it will be retained
  - Include instructions for exercising individual rights (such as access)
  - French law requires you to indicate if the data will be transferred outside the EEA, and (if so) the authority for the transfer



## Notice and Consent Forms – General Requirements

- Notice and consent forms must be written in a language that the candidate reads easily
  - French law requires that the notices be in French, even if the candidate is fluent in another language
- Consent forms must be very specific – overbroad “blanket” consent forms are generally not enforceable in countries with DP laws
  - Consents must be specific as to transaction as well as to the searches to be conducted



## Individual Rights

- Individual rights under DP laws are perhaps the most consistent with US screening laws
- As with the FCRA, individuals have the right to receive notice and exercise choice
- Individuals also have the ability to access and correct information about them used in screening processes
- Processes used to comply with FCRA rights may be leveraged to meet international requirements



## Data Transfers

- If data will be transferred from Europe or other jurisdictions with transfer restrictions, authorization for transfers will need to be considered
  - In Japan, consent for the transfer must be obtained from the candidate
- In Europe, processors must rely on controllers to authorize the transfers
  - Controllers may permit the transfer based on a Safe Harbor certification
  - Controllers may rely on Model Contracts
  - If the data subject in the EU is seeking a job outside of the EU, consent may be appropriate



## Session 3 Conclusions

- Begin by identifying the applicable requirements, based on the locations of the candidate and the job
- Consider published advice where available to help understand how the rules should be applied
- Leverage US processes where possible (such as access) – but realize that international laws will likely demand new processes that are fundamentally different from the ones you use in the United States

