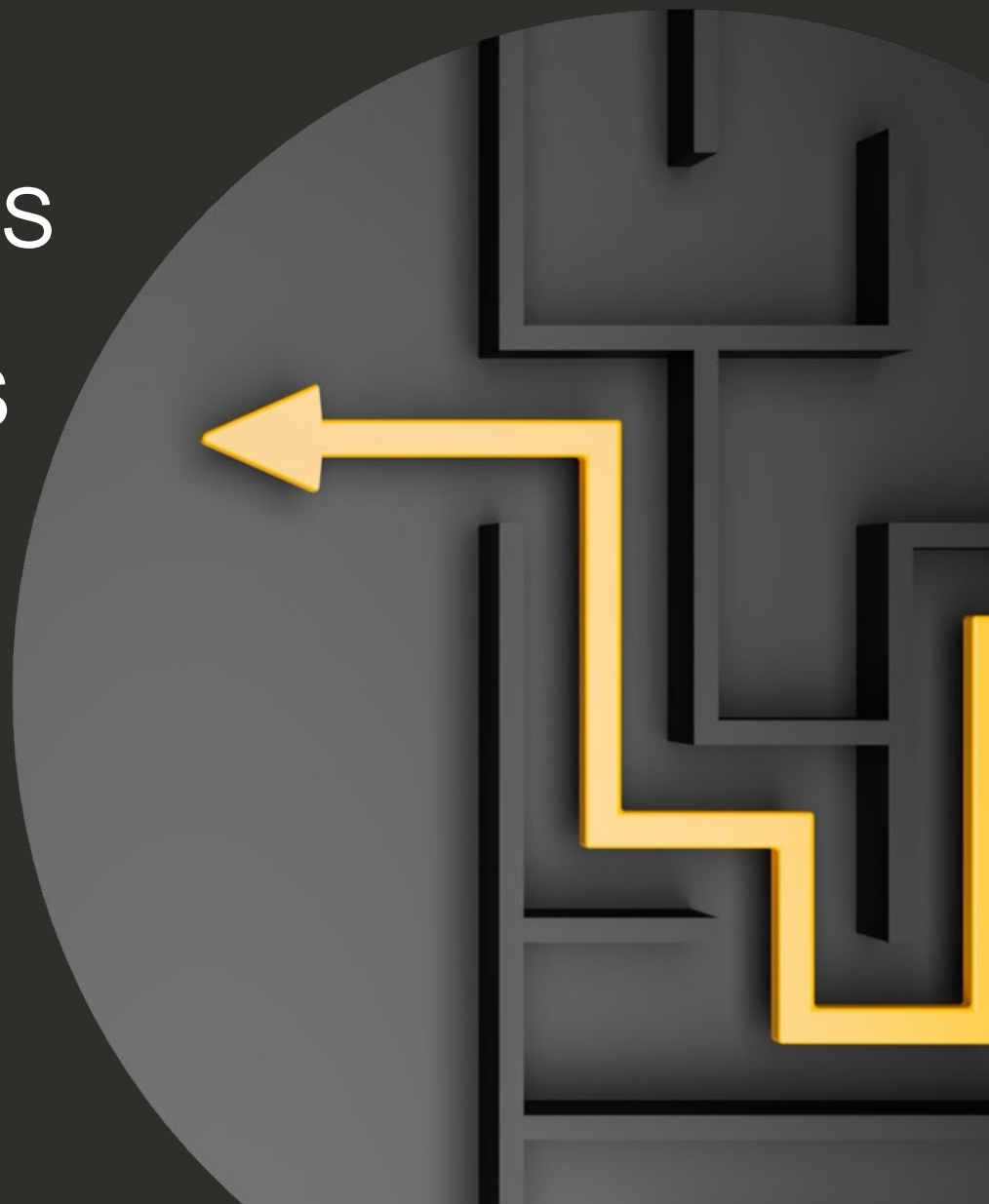
ENFORCEMENT OUTLOOK SERIES

DATA PRIVACY CONSIDERATIONS IN INTERNATIONAL INVESTIGATIONS

SIMON AIREY (PARTNER, LONDON)

DAVID SAUNDERS (PARTNER, CHICAGO)



McDermott Will & Emery

9 November 2022

mwe.com

PRESENTERS

SIMON AIREY

Partner

+44 (0)20 7577 3470 | sairey@mwe.com

Simon Airey focuses his practice on global, cross-border and internal investigations, financial and regulatory crime, bribery and corruption, money laundering, tax and fraud inquiries, data breaches, dawn raids, asset tracing, international enforcement and corporate compliance issues

DAVID SAUNDERS

Partner

+1 312 803-8305 | dsaunders@mwe.com

David Saunders is a Partner in McDermott Will & Emery's Global Privacy & Cybersecurity practice. Through the lens of a litigator, Mr Saunders helps clients navigate their risks in the data privacy and cybersecurity arenas

INTRODUCTION

- In the heat of an internal investigation, it is easy to focus on speed / progress and ‘overlook’ data privacy

- However, every investigation will likely involve the processing of personal data of (a) current and former employees and (b) third parties, especially in relation to:
  - data preservation, collection and review
  - dealing with data held overseas
  - transferring data between jurisdictions
  - producing data to law enforcement authorities or the courts

- Breach of the rules can result in regulatory scrutiny, financial sanctions and even criminal liability

- Potential for conflict between rules / obligations, especially in cross-border context

OUTLINE OF TODAY'S SESSION

- Legal considerations
  1. Which jurisdictions' rules apply?
  2. Key risk areas
  3. Consequences of getting it wrong

- Practical tips
  1. Avoiding common jurisdictional pitfalls
  2. General best practice
  3. Negotiating with authorities
  4. Attorney-client / legal privilege

LEGAL CONSIDERATIONS

EXAMPLES: CROSS-BORDER INVESTIGATIONS

Investigation	Investigating agencies (non-exhaustive)	Relevant jurisdictions (non-exhaustive)
Aircraft engine manufacturer	US, UK, Brazil	Indonesia, Thailand, India, Russia, Nigeria, China, Malaysia, Brazil, Kazakhstan, Azerbaijan, Angola, Iraq
Airplane manufacturer	US, UK, France	Sri Lanka, Malaysia, Indonesia, Taiwan, Ghana, China, Colombia, Nepal, India, South Korea, UAE, Saudi Arabia, Taiwan, Russia, Vietnam, Austria, Japan, Turkey, Mexico, Thailand, Brazil, Kuwait
Financial services	US, UK, Switzerland, European Commission (anti-trust)	UK, USA, Germany, Japan, Switzerland, Hong Kong, Singapore
AI surveillance	US, Australia, France, UK	EEA, US, Australia, Canada
Financial services	US, UK, Denmark	Denmark, Estonia, UK, USA

PATCHWORK OF US PRIVACY LAWS

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Federal Trade Commission Act (FTC)
- Other Federal Laws
  - Children's Online Privacy Protection Act (COPPA)
  - Gramm-Leach-Bliley Act (GLBA)
  - Fair Credit Reporting Act (FCRA)
  - Common Rule (Federal Policy for the Protection of Human Subjects)
- State Laws
  - Constitutional Right of Privacy
  - State laws protecting confidentiality of general health information
  - State laws protecting sensitive categories of personal health information (e.g., genetic, biometric, HIV AIDS, mental health)
  - State Data Breach Notification Laws
  - State Consumer Protection Laws (e.g., California Consumer Privacy Act)
  - Common Law Case Law

Different collaborators, technologies and data sources may trigger an intersection of Privacy, Consumer Protection and related laws and public policies

EXAMPLES OF REGULATED DATA IN THE US

Medical Data

- Data created, received, stored, or transmitted in relation to the provision of healthcare (e.g., patient data)
- Full data rights (including written consent) and state and federal statutes will apply

Employee Data

- Data about employees, job applicants, directors, officers, and medical staff members collected in the context of that relationship
- Typically limited data rights but requirements for notice, transparency and reasonable security

Business Contact Data

- B2B marketing lists and other contact lists about employees of entities with which an organisation partners
- Typically limited data rights but requirements for opting out of sale (i.e., the exchange of data for consideration or benefit – monetary or otherwise)

Consumer Data

- Data about website users and consumers that interact with the organisation
- Full data rights and requirements of the consumer privacy statute will apply

JURISDICTIONAL REACH OF GDPR

- The GDPR and UK GDPR apply to:

  1. organisations that have an **establishment** in the UK / EU and process data in the context of the activities of that establishment; or

  2. organisations that **offer goods or services** to, or **monitor,** data subjects in the UK / EU

- In scenario (1), the key question is whether there is an establishment

  – Covers subsidiaries, branches, offices and even a single permanent representative

  – It is irrelevant where the data subjects are located or where the processing takes place

- In scenario (2), key question is whether UK / EU customers are targeted or monitored

OTHER KEY JURISDICTIONAL RULES

Jurisdiction	Rule
France	**Blocking statute** prohibits disclosure of 'sensitive information' for use in foreign proceedings
Switzerland	Numerous **restrictions** on disclosure of personal or financial data to foreign courts, regulators or enforcement authorities, or even internal disclosures amongst affiliates
Germany	General **prohibition** on companies accessing **employees' private data** (unless good reason to do so) If employees use work accounts to send private messages / emails, corporate can be deemed a 'telecoms service provider', triggering additional **secrecy laws** (breach of which is a criminal offence) Requirement for works council consultation
Israel	Restriction on international data transfers unless the receiving country ensures **a level of protection at least equal** to that under Israeli law; data localization issues
China	**New data protection** law has undeveloped mechanisms for cross-border transfer of personal data

DOCUMENT PRESERVATION, COLLECTION AND REVIEW

- Ensuring relevant documents are preserved is of critical importance
  - In certain cases, failure to do so can be a criminal offence
  - Document preservation notices
  - IT ‘holds’; consider where the data can or has to be stored
  - Limit access to the information
- Under (UK) GDPR, need a ‘lawful basis’ to process data
  - Beware reliance on ‘consent’
  - ‘Legitimate interests’ balancing exercise
  - Principles of transparency, data minimisation and storage limitation

INTERNATIONAL DATA TRANSFERS

- Touchstone questions
  - Is it necessary?
  - Is it legally permitted?
- The need for data to be transferred across borders can arise frequently during investigations
  - Data held on cloud-based servers physically located overseas
  - Sharing information with external advisors in other jurisdictions
  - Productions to overseas law enforcement authorities or courts
- Consider local law advice as to whether data can be transferred out of the jurisdiction
- Is there an appropriate transfer mechanism in place?

PRODUCTION TO AUTHORITIES

- Need to consider data protection rules of both (a) original country of data collection and (b) country of production
- (UK) GDPR
  - If producing subject to a subpoena / production order
    - "*processing is **necessary** for compliance with a **legal obligation** to which the controller is subject*"
  - If producing voluntarily:
    - "*processing is **necessary** for the purposes of the **legitimate interests** pursued by the controller or by a third party, **except where such interests are overridden** by the interests or fundamental rights and freedoms of the data subject*"
  - Additional requirements for 'special category data'
- Is redaction possible / feasible?

PRODUCTION TO AUTHORITIES

- USA
  - Different mechanisms that permit production without risk of further dissemination or waiver of privilege
  - Government authorities will frequently start from the proposition that they are entitled to everything
    - Not always mindful of international privacy implications of request
  - Negotiation of what will be delivered is often the hardest part of the process
  - Context is often important
    - Criminal v civil
    - Victim v alleged bad actor

CONSEQUENCES OF GETTING IT WRONG

- Breach of (UK) GDPR can result in fines of **up to 4%** of total annual worldwide turnover in preceding year
- Breach of US data privacy rules can lead to regulatory penalties, fines, injunctive relief and private lawsuits
- How likely is enforcement?
  - Will the organisation be caught?
  - Even if caught, will the organisation realistically face sanction?
  - Possible issues with admissibility of evidence
- Risk-based approach

KEY PRACTICAL TIPS

AVOIDING JURISDICTIONAL PITFALLS

- Consider the possibility of an international dimension or repercussions at the outset
- Do not assume that laws in all countries are the same or similar or that, because it's a group company, it's your data and the rules don't apply
- Note that the attitudes and approach of foreign law enforcement agencies and regulators can differ significantly
- Consider obtaining local advice / input at the outset
- Be aware of differing local approaches to privilege

GENERAL BEST PRACTICE

- Identify location of server data and location of data subjects
- Evaluate need to localise data and precursors to collection of data
- Identify any ‘special category data’ at point of review / before production
- Document justification for each distinct type of data processing
- Redact particularly sensitive information where possible
- Exercise tight control over data access rights / permissions; consider privilege implications
- Seek to refer to data processing as part of possible investigations in employment contracts / employee privacy notices
- When an investigation arises, consider appropriate transparency (e.g., when circulating hold notices)

NEGOTIATING WITH AUTHORITIES

- Concern that ‘data privacy’ may be used as an excuse
- Inappropriate claims can lose credibility
- What if there is a genuine conflict between the expectations of authorities and overseas data privacy laws?
  - Risk-based approach
  - Alternative route? Mutual legal assistance / letters of request?

“Corporations are often too quick to claim that they cannot retrieve overseas documents, emails or other evidence regarding individuals due to foreign data privacy laws […] A company that tries to hide culpable individuals or otherwise available evidence behind inaccurately expansive interpretations of foreign data protection laws places its cooperation credit at great risk”

(US Department of Justice, September 2014)

ATTORNEY-CLIENT PRIVILEGE CONSIDERATIONS

	United States	United Kingdom	France
Is a privilege waiver required?	Waiver not required but can be a positive consideration	Waiver is not required but is viewed as a positive indication of cooperation	Withholding privileged material can be viewed as uncooperative
Is cooperation with international agencies relevant?	Highly relevant to determination of cooperation	Encouraged but unclear if it is a mitigating factor	Encouraged but French law and guidance may hinder efforts to do so

THANK YOU / QUESTIONS?

mwe.com