

# Draft Outline - Managing the tension between government information requests and data protection obligations in the Middle East context



**The Sedona Conference**  
**Working Group 6 – Middle East Committee**  
**DRAFT COMMENTARY OUTLINE v2**

**Working title:** "Managing the tension between government information requests and data protection obligations in the Middle East context"

**Drafting leads:** Dino Wilkinson, Lori Baker

**Summary and objectives:** Commentary on the conflict faced by organisations in the Middle East between legal and quasi-legal requirements to disclose personal data to governmental (and other) authorities and the burgeoning data protection regimes in the region.

Key objectives of the paper are to provide context and commentary on issues specific to the Middle East and practical guidance for legal and compliance professionals on handling these conflicts and mitigating risks.<sup>1</sup>

**Outline:**

1. Introduction
  - a. Setting the scene
    - i. Typical Middle East data disclosure requirements and request procedures (nb. often "informal", no subpoena or similar, unclear whether authority is acting within its powers). Examples would include requests from municipal authorities for details of conference delegates and speakers or requests from security authorities for guest data from a hotel.
    - ii. Proliferation of new and developing data protection regimes (new laws in Bahrain, Lebanon; new regulatory authorities in Qatar, Bahrain; consultations in Egypt, Jordan, DIFC; reported developments in UAE, Saudi Arabia, Oman). Cite to prior working papers by this Committee or sources from WG6 ME bibliography.
    - iii. Distinctions on types of data – personal/sensitive, data classification rules, uncertainty over classification or definition: see "government information" (e.g. as referred in Saudi Arabia Essential Cybersecurity Controls), "confidential information"/"information about a person's private or family life" (UAE Penal Code).
  - b. Establishing the issue(s)
    - i. Conflict between data disclosure requests and data protection principles (including data exports in the case of free zone companies disclosing to onshore regulators).
    - ii. Explanation of how this issue is different to (or more acute than) Europe/US:

---

<sup>1</sup> A core function of The Sedona Conference is to develop non-partisan consensus commentaries that provide guidance of immediate practical benefit to the Bench and Bar.

1. Different regulatory approaches, often "informal" and unclear – substantially less process (and accountability?) than Europe/US
  2. National security focus – geopolitical issues
  3. Data classification?
  4. Absence of formal systems of precedent or published case law.
2. Detailed commentary
- a. Assessment of key issues
    - i. Reference to specific DP regimes (see overview at the end of the Sedona Choice of Law paper (2018 International Programme reading materials) and Lori/Julie's draft paper)
  - b. Applying best practice international approaches
    - i. [EU/Japan adequacy decision](#) – especially section 3 (access and use of personal data by public authorities in Japan) and Annex 2 (overview of the legal framework concerning access to information by the government of Japan)
    - ii. [UK ICO consultation on draft data sharing code of practice](#)
  - c. New/developing approaches
    - i. See [Article 28](#) of DIFC consultation draft Data Protection Law which seeks to place obligations on the controller to consider and balance the competing requirements.
      1. Consider examples in practice, e.g. if this were before a US court and a protective order could not be obtained, or if motions to limit or narrow overly broad discovery requests were denied, then under Article 28 a party could refuse to produce/disclose under DIFC law, but what would happen before the US court?
    - ii. [Lori to obtain approval to share DIFC government data sharing policy – based on Japan decision requirements in Annex 3 and ICO/Australia data sharing guidance]
3. Practical tips
- a. Summary of practical guidance, including:
    - i. Assessment and due diligence by the controller in respect of any request
    - ii. Assess risk of proposed transfer
    - iii. Transparency – even if few risk mitigations available, must be clear that such transfers can and do take place.
    - iv. Consider measures to minimise or mitigate risk – see Sedona principles and practical guidance paper, but this paper can go further including:
      1. Redaction or minimisation of personal data (Jerami has experience of funnel diagrams used to show each stage where culling/minimisation occurs; also decision logs used as part of a

legitimation plan that bolsters both accountability and a position to put forward to the requesting authority)

2. Engaging data protection authority for guidance? cf. Challenges in underdeveloped DP jurisdictions, v limited experience of regulators and little/no guidance available.
3. Seeking binding assurances from requesting party