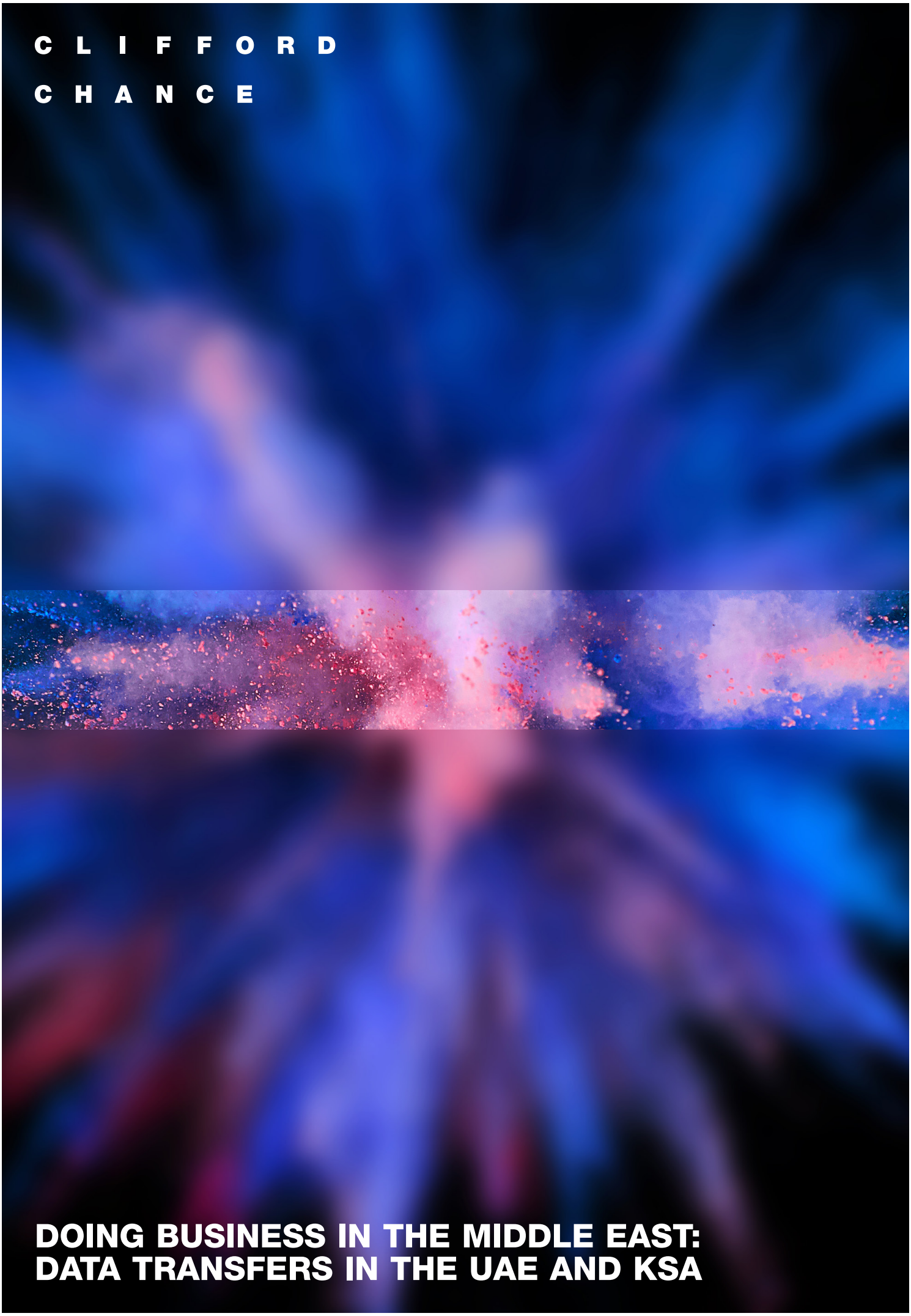
CLIFFORD
CHANCE



DOING BUSINESS IN THE MIDDLE EAST: DATA TRANSFERS IN THE UAE AND KSA

DOING BUSINESS IN THE MIDDLE EAST: DATA TRANSFERS IN THE UAE AND KSA

In today's information economy, the ability to transfer data across borders is fundamental to doing business and accelerating growth. This short guide sets out an overview of the key legal and regulatory requirements regarding cross-border data transfers in the United Arab Emirates (UAE), the UAE's financial free zones (the Dubai International Financial Centre (DIFC) and the Abu Dhabi Global Market (ADGM)) and the Kingdom of Saudi Arabia (KSA).

When doing business in the UAE and the KSA, there are two types of restrictions that you must consider before transferring data across borders:

1. Personal data protection laws; and

2. Data localisation requirements.[1]

Personal Data

The rules on transfers of personal data are dependent on the applicable data protection regime. In the region, the following key laws have provisions regarding cross-border data transfers:

- **UAE** – Federal Decree-Law No. 45 of 2021 Concerning the Protection of Personal Data (**UAE DP Law**). There are two key points to note regarding the UAE DP Law:

  – The law does not apply to all types of personal data. It does not regulate: (i) government data, (ii) data processed by government entities, security or judicial authorities, (iii) personal health data, or (iv) personal banking and credit data. In the case of (iii) and (iv), these data types are instead regulated under other federal legislation as noted under the data localisation section below.

  – Whilst the law came into force on 2 January 2022, various aspects of the UAE DP Law are still expected to be clarified in the impending executive regulations. The executive regulations were expected to be released in March 2022, however, these are yet to be released and there is no indication of when such executive regulations may be published. Controllers and processors of personal data must comply with the UAE DP Law within a period of six months from the date of issuance of the executive regulations (although this period may be extended).

- **DIFC** – DIFC Data Protection Law No. 5 of 2020 (**DIFC DP Law**)

1 Businesses, in particular financial institutions, should note that in addition to the cross-border transfer requirements described in this article, when sharing data with third parties they will need to comply with additional requirements regarding third party disclosures, such as banking secrecy, outsourcing and confidentiality rules.

- **ADGM** – Data Protection Regulations 2021 (**ADGM DPR**)
- **KSA** – the Personal Data Protection Law (and its Regulation on Personal Data Transfer outside the Kingdom (**Data Transfer Regulation**)).

Under all these regimes, personal data is defined broadly – it includes any information relating to an identified or identifiable natural person. For example, individual customer or employee data. It does not include data relating to legal persons, such as companies.

Generally, the requirements on businesses regarding cross-border transfers align with approaches that may be familiar under other data protection laws globally, particularly under the GDPR. There are several permitted ways of transferring personal data across border:

- **Adequacy Decision** – Transfers of personal data may take place to countries that are deemed by the local data protection authority to provide an adequate level of protection for personal data. This list is typically maintained on the website of the local regulator/authority.

- **Appropriate safeguards** – Transfers to countries that are not deemed 'adequate' may still be undertaken as long one of the safeguards specified under the relevant law has been implemented. These include:

  – **Standard Contractual Clauses** – These are standard form contractual terms that are issued by the local data protection authority that must be completed and signed by both parties. This is the most popular method used by businesses for cross-border transfers to non-'adequate' jurisdictions. The clauses impose contractual obligations on the sender and the receiver of the data, and grant rights to people whose personal data is transferred.

  – **Binding Corporate Rules** – This is an internal policy that businesses may put in place for intragroup transfers, the form of which may require approval by the regulator.

  Other examples may include certifications and binding codes of conduct. In addition, it is often necessary to conduct a risk assessment to identify if any further measures need to be taken to ensure the appropriate protection of the personal data.

- **Derogations or exemptions** – As a last resort, in some limited instances a transfer may still be able to take place relying on a derogation or exemption under the applicable data protection regime. However, these are not to be routinely relied on.

A detailed list of the requirements is set out in Table 1.

Table 1 – Summary of data transfer requirements under UAE and KSA data protection laws

	Which jurisdictions are deemed 'adequate' under local data protection laws? Adequate jurisdictions (as of 5 March 2025)	Can I rely on 'appropriate safeguards'?		Are there any additional requirements?
		Standard Contractual Clauses?	Binding Corporate Rules?	
UAE	The competent authority regulating matters covered by the UAE DP Law, the UAE Data Office, is still in the process of being set up, thus, a list of 'adequate' jurisdictions is yet to be published.	✗ – However, whilst no standard contractual clauses have been published for use in the UAE, in practice, businesses often rely on the published EU SCCs.	✗	To be confirmed once the executive regulations are published.
DIFC	The full list of 'adequate' jurisdictions are set out here, and include: • All EEA countries • UK • Canada • Singapore • ADGM • Japan • California • Republic of Korea	✓ – available here	✓	In the absence of an adequacy decision or an appropriate safeguard, there are limited derogations set out in the DIFC DP Law. For example, where: • you obtain explicit consent from the data subject (after being informed of the risks); • the transfer is necessary for the performance of a contract between the data subject and controller; or • the transfer is necessary for the performance of a contract between controller and third party (in the interests of the data subject). When sharing data with government authorities, you will need to obtain written assurances for handling personal data in line with applicable data protection law or carry out a self-assessment of risk, necessity and proportionality.

	Which jurisdictions are deemed 'adequate' under local data protection laws? Adequate jurisdictions (as of 5 March 2025)	Can I rely on 'appropriate safeguards'?		Are there any additional requirements?
		Standard Contractual Clauses?	Binding Corporate Rules?	
ADGM	The full list of 'adequate' jurisdictions are set out here, and include: • All EEA countries • UK • Canada (provided recipient is subject to the PIPED Act) • DIFC • Japan	✓ – available here	✓	In the absence of an adequacy decision or an appropriate safeguard, there are limited derogations set out in the ADGM DPR. For example, where: • you obtain explicit consent from the data subject (after being informed of the risks); • the transfer is necessary for the performance of a contract between the data subject and controller; or • the transfer is necessary for the performance of a contract between controller and third party (in the interests of the data subject).
KSA	A list of 'adequate' jurisdictions has not yet been published by the SDAIA. Until such list is published, SCCs may be the most advisable method to effect transfers of personal data outside of the KSA.	✓ – available here	✓	There are limited exemptions set out in the Data Transfer Regulation. A risk assessment must also be conducted where a controller is using appropriate safeguards to transfer personal data outside of KSA or where sensitive data is being transferred to entities outside KSA on a continuous or widespread basis (or where the processing more generally meets the risk assessment criteria under the Implementing Regulation).

Non-compliance with data protection laws in the region may result in fines and, in some cases, criminal penalties.

Data Localisation

In addition to obligations under personal data laws, local laws may prohibit businesses from transferring certain data types outside of the country. Over the years, data localisation requirements have generally been relaxed in the region. However, in limited cases they still apply and where they do, businesses may have to make alternative provisions to ensure compliance (e.g. storing data in local data centres in the relevant jurisdiction). Non-compliance may result in fines, suspension of services and, in some cases, criminal penalties.

Further, it is worth noting that even where these provisions do not apply to businesses directly, they may be indirectly relevant to your business to the extent that you are a service provider or store data on behalf of customers that are subject to these requirements.

Below, we have set out some examples of the key data localisation requirements in the region:

UAE

- **Banking** – The UAE Central Bank's Consumer Protection Standards (2021) requires all licensed financial institutions to store customer and transaction data within the UAE. Central Bank approval and consent of the customer may be required for cross-border transfers.

- **Payment Services** – The UAE Central Bank's Retail Payment Services and Card Schemes Regulation (2021) imposes data protection obligations on entities providing retail payment services or operating card schemes in the UAE and provides that personal and payment data must be stored and maintained in the UAE.

- **Healthcare** – Federal Law No. 2 of 2019 Concerning the Use of the Information and Communications Technology in Health Fields (also known as the 'Healthcare ICT Law') requires electronic health data to be stored in the UAE and primarily applies to healthcare providers, health authorities and insurance providers, subject to certain exceptions.

- **Internet of Things** (**IoT**) – The Internet of Things Regulatory Policy (22 March 2018) requires that certain IoT service providers store categories of data determined as 'secret', 'sensitive' and/or 'confidential' in the UAE or only in countries that meet or exceed the data security requirements in the UAE. If the data is 'secret', 'sensitive' and/or 'confidential' and also relates to the government, such data must remain in the UAE at all times.

KSA

As a preliminary point, in October 2024, the Saudi National Cybersecurity Authority released the Essential Cybersecurity Controls 2024 (**ECC-2**). The most significant changes that the ECC-2 has introduced was the removal of the requirements for governmental entities and those owning, operating or hosting critical national infrastructure to store data within KSA. However, the following localisation requirements remain in place:

- **Government Data** - the Cloud Computing Services Provisioning Regulations require businesses (termed 'Subscribers' under the law) whose data is classified as data of Saudi government agencies to use cloud service providers registered with the Communications & Information Technology Commission (and are therefore located in the KSA).

- **Banking** – The Saudi Arabian Monetary Authority's (**SAMA**) Cybersecurity Framework may require the approval of SAMA where cloud services located outside of the KSA are used by SAMA registered entities.

- **Capital Markets** – The Capital Market Authority's (**CMA**) Cybersecurity Guidelines for Capital Markets Institutions require cloud-computing services used by CMA registered entities to be located in the KSA.

- **Insurance** - The Insurance Market Code of Conduct Regulation requires insurance companies to maintain customer personal data in the KSA.

- **Employment** - The Labor Law requires that certain records, statements and files are maintained at the workplace whether in hard or soft copy.

CONTACTS

If you have any questions, please do not hesitate to contact our regional experts using the details below.

Jack Hardman
Partner
Dubai
T: +971 4503 2712
E: jack.hardman@cliffordchance.com

Selman Ansari
Counsel
Riyadh (AS&H Clifford Chance)
T: +966 11 481 9735
E: selman.ansari@ashcliffordchance.com

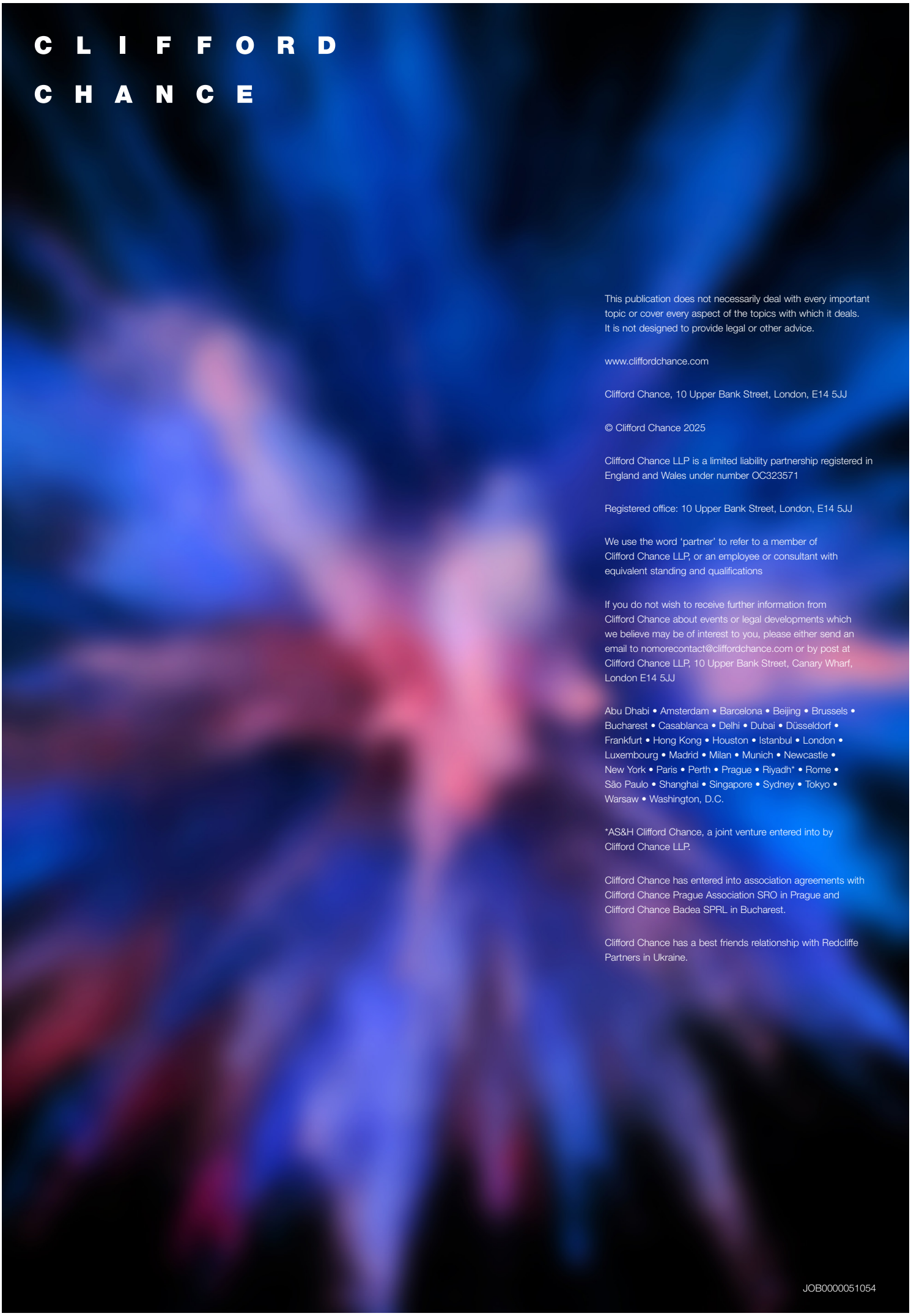
Adam Hunter
Associate
Dubai
T: +971 4503 2602
E: adam.hunter@cliffordchance.com

Sami Rahim
Associate
Dubai
T: +971 4503 2758
E: sami.rahim@cliffordchance.com

Tosin Murana
Associate
Dubai
T: +971 4503 2788
E: tosin.murana@cliffordchance.com

Mehran Azzam
Associate
Abu Dhabi
T: +971 2 613 2318
E: mehran.azzam@cliffordchance.com

Muath Alsowayan
Associate
Riyadh (AS&H Clifford Chance)
T: +966 114819769
E: muath.alsowayan@ashcliffordchance.com



CLIFFORD
CHANCE

JOB0000051054