OPINION

UNDERSTANDING DATA PROTECTION: A GUIDE FOR PRIVATE STRUCTURES IN THE DIFC AND THE ADGM

In every structure, whether a holding company, a special purpose vehicle, family office, or advisory firm, Personal Data[1] operates as a silent stakeholder. It surfaces in shareholder registers, board minutes, passport copies, email trails, and service contracts. It holds value, creates exposure, and requires clear accountability.

Managing Personal Data is not a box-ticking exercise. It is a **governance obligation**. Treating Personal Data as a stakeholder means protecting individual rights, minimising risk, and fostering trust, not just with regulators, but with counterparties, clients, and family members.

DATA PROTECTION FOR ALL

Sophisticated data protection regimes have been adopted in both the Abu Dhabi Global Market (the "**ADGM**")[2] and the Dubai International Financial Centre (the "**DIFC**")[3]. These frameworks are modelled on international best practice, including the General Data Protection Regulation ("**GDPR**") of the European Union[4], which sets a global benchmark for Personal Data governance and individual rights. In both jurisdictions, **the rules apply to all registered entities that process Personal Data**. This includes **passive holding structures**, such as **special purpose vehicles** and **foundations**, as well as privately controlled entities like **family offices** and **proprietary investment companies** that manage or coordinate Personal Data in connection with legal affairs or assets.

Entities with no employees or active operations may still hold, transmit, or delegate control over personal information. This triggers data protection obligations, including registration, ongoing documentation, and internal governance requirements. However, there is a common misconception that data protection rules and obligations do not apply to these entities.

Even passive vehicles typically process some level of Personal Data, whether through routine filings, correspondence, or service provider interactions. Where Processing[5] occurs, obligations are triggered. Overlooking these requirements exposes these entities to compliance failures and potential penalties.

1. As defined in the Comparison Table attached as Annexure 1.
2. *Abu Dhabi Global Market Data Protection Regulations 2021, Abu Dhabi Global Market ("**ADGM DP Regulations**").*
3. *DIFC Law No. 5 of 2020, Data Protection Law, Dubai International Financial Centre ("**DIFC DP Law**").*
4. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, pp. 1–88.*
5. As defined in the Comparison Table attached as Annexure 1.

DIFC VS ADGM FRAMEWORKS

While the ADGM and DIFC frameworks are closely aligned—both drawing heavily from GDPR principles—their differences are more nuanced than sweeping. In practice, the regimes impose almost identical obligations around lawful bases, registration, breach notification, data transfers, and Processor[6] oversight. **Annexure 1** contains a comparison table (the "**Comparison Table**") highlighting distinctions and commonalities, offering a practical overview to help entities understand where their compliance approach may need to be tailored to each jurisdiction.

WHY DATA PROTECTION MATTERS

Both ADGM and DIFC frameworks are grounded in the protection of fundamental rights, including the right to access Personal Data, correct inaccuracies, object to certain types of Processing, and request deletion. The obligation to protect these rights apply equally to all entities, (big or small, active or passive) that process personal information.

As Giovanni Buttarelli, the former European Data Protection Supervisor, observed: *"Data protection came in response to the growing …ability to collect and use large amounts of information, and the profitability of collecting and using… data [which has] consequences for individual freedom and privacy."*[7] This concern sits at the core of modern governance frameworks. As data becomes increasingly valuable and monetised, protecting privacy is no longer just a matter of regulatory compliance (and avoiding penalties), it is a reflection of institutional integrity and respect for individual rights.

"Protecting privacy is no longer just a matter of regulatory compliance (and avoiding penalties), it is a reflection of institutional integrity and respect for individual rights."

The risks of failing to do so are well established. In the Cambridge Analytica scandal, data from over 87 million Facebook profiles was harvested and used without consent to influence voter behaviour. The fallout included a USD 5 billion fine for Facebook by the US Federal Trade Commission, parliamentary inquiries across jurisdictions, and lasting reputational damage to all parties involved.[8] These events reshaped the global conversation on data protection and remain a key reference for regulators.

6. As defined in the Comparison Table attached as Annexure 1.
7. Buttarelli, Giovanni, 40th ICFPPC: Opening Speech, Choose humanity: Putting dignity back into Digital, 40th ICDPPC: Opening Speech by Giovanni Buttarelli.
8. Investigation into the use of data analytics in political campaigns.

Structures created to preserve wealth, continuity, or reputation must also preserve rights. This does not require flawless systems or absolute coverage. What is required is a structured, well documented, and proportionate approach to governance, that reflects the nature of the entity, the sensitivity of the data, and the risks involved.

Treating data as a stakeholder builds trust, supports long-term success, and reduces legal and reputational risk. This is not just about following rules. It is about doing what is right.

DATA PROTECTION IN PRACTICE

Compliance requirements for a private operational company such as a single-family office ("**SFO**") are far more demanding than for a passive holding entity, such as a special purpose vehicle ("**SPV**"). The SPV, with no staff or active operations, typically only needs to meet baseline obligations — maintaining Records of Processing Activities ("**ROPA**"), putting in place Processor agreements with their corporate service provider ("**CSP**"), documenting their decision not to appoint a Data Protection Officer ("**DPO**") or conduct Data Protection Impact Assessments ("**DPIAs**"), and ensuring cross-border transfers are safeguarded. By contrast, the SFO processes far greater volumes and more sensitive categories of Personal Data, and engages multiple external vendors. The sensitivity of the Personal Data collected, means its compliance obligations extend well beyond the minimal framework expected of the SPV.

The following case studies show what to do, what to avoid, and how to stay compliant.

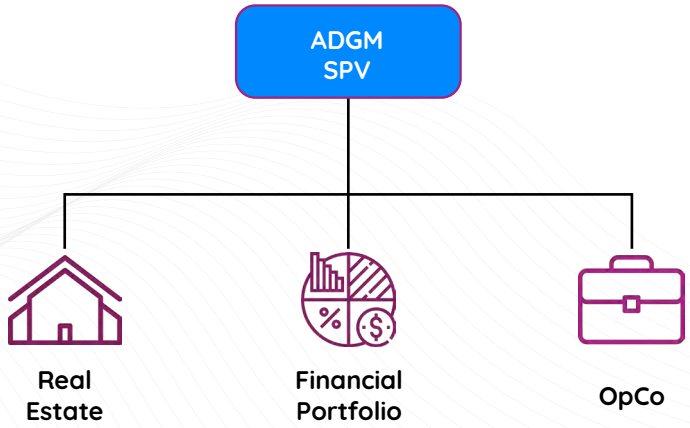
CASE STUDY 1: PASSIVE SPECIAL PURPOSE ENTITY ESTABLISHED IN THE ADGM

Background

A SPV is established in the ADGM to consolidate family-held assets, including real estate, portfolio investments, and shares in an underlying operational company. The SPV by its nature, is a passive holding entity, not permitted to employ staff or conduct business.

Personal Data such as passport copies, national ID cards, residential addresses, bank details, and other identifying information, relating to the ultimate beneficial owners, directors, shareholders, and authorised signatories is maintained by the SPV.

In accordance with ADGM regulations, the SPV appoints a licensed CSP to provide a registered address and undertake administrative filings. As part of onboarding and ongoing administration of the SPV, the CSP collects and processes this Personal Data, including sharing it with the ADGM Registration Authority to meet annual compliance requirements.



Case Study 1 - Typical Compliance Gaps

- Unclear roles and missing paperwork. In practice, many SPVs act as the Controller[9] while the CSP is the Processor, but there is often no detailed contract setting out responsibilities such as following instructions, keeping data secure, managing sub-Processors, assisting with rights requests, or returning and deleting data when the engagement ends.
- Not giving shareholders, directors and UBOs clear and accessible information about how their Personal Data is handled. For example, notices that fail to explain clearly why Personal Data is collected, how it will be used, and with whom it will be shared.
- Records of Personal Data are often kept longer than necessary, especially copies of IDs or bank details, instead of being deleted or restricted once the purpose is complete.
- No proper data transfer mechanisms when using systems or service providers outside the ADGM.
- Not having a clear process for data breaches, and overlooking the need to assess whether specific risk governance measures apply.

Case Study 1 - Best Practice Approach

To close these gaps, the SPV should:

i. **Clarify roles** – who is the Controller and who is the Processor.

ii. **Implement a Data Processing Agreement** with the CSP.

iii. **Maintain a ROPA.**

iv. **Ensure a lawful basis** is identified and documented for all Processing activities.

v. **Provide privacy notices** to Data Subjects[10] to explain why Personal Data is collected, how it will be used, and with whom it will be shared.

vi. **Ensure appropriate controls on cross-border transfers**.

vii. **Adopt a breach response plan** that enables it to notify the Commissioner within 72 hours of becoming aware of a Personal Data Breach and to communicate without undue delay with affected individuals if their rights are at high risk.

9. As defined in the Comparison Table attached as Annexure 1.
10. As defined in the Comparison Table attached as Annexure 1.

"Even a passive SPV with limited scope remains subject to Controller obligations under the ADGM DP Regulations."

Even a passive SPV with limited scope remains subject to Controller obligations under the ADGM DP Regulations. At a minimum, it must maintain a ROPA, formalise Processor agreements with its CSP, and ensure that cross-border transfers are properly safeguarded.

Documenting decisions—such as why no DPO or DPIA[11] is required—and adopting a proportionate breach response plan are equally important. By addressing these baseline requirements proactively, an SPV can minimise regulatory risk and avoid liability being redirected back to it.

11. A passive holding SPV with no staff will generally not engage in high-risk or large-scale Processing of Personal Data, and therefore will not typically be required to conduct a data protection impact assessment or appoint a data protection officer. However, it should document this conclusion and review it periodically, particularly if its activities expand.

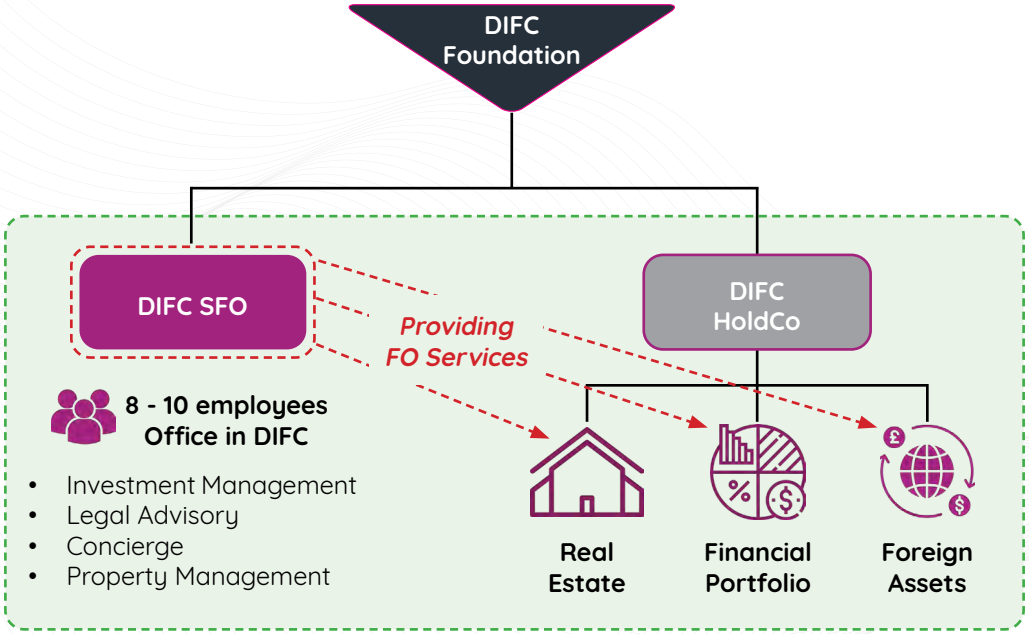
CASE STUDY 2: OPERATIONAL SINGLE FAMILY OFFICE ESTABLISHED IN THE DIFC

Background

A SFO is registered in the DIFC to provide investment management, legal advisory, concierge, and property management services to one family across two generations. The SFO employs 8–10 people and maintains an office in the DIFC.

Extensive personal and financial data of family members, including minors, is held and managed by the SFO. Travel records, medical appointments, legal documentation, property files, employment records, and vendor details are regularly processed.

Data is handled by multiple internal team members and external providers (wealth managers, recruiters, legal counsel, concierge agents) inside and outside the UAE. Data is stored in shared drives.



Case Study 2 - Typical Compliance Gaps

The main challenges arise from the nature and volume of Special Categories of Personal Data being processed. Health records, legal files, and travel documents (to the extent the latter two contain such sensitive data[12]) all fall within Special Categories of Personal Data[13] under the DIFC regime, yet many SFOs do not obtain or document explicit consent or identify another proper lawful basis for handling them. Children's information is often treated in the same way as adult family members' data, without enhanced notices or safeguards – which is good practice for data processed in the DIFC.

Sensitive records are also commonly stored in shared drives with broad access and limited security controls, increasing the risk of inappropriate access or loss. Oversight of external providers, such as wealth managers, recruiters, legal counsel and concierge agents, is inconsistent. Many of these service providers operate without contracts that reflect the DIFC's Processor and sub-Processor requirements whereby such contracts must, at a minimum, set out that Processors act only on documented instructions, apply appropriate security measures, ensure confidentiality, engage sub-Processors only with authorization, assist with Data Subject rights and breach notifications, and return or delete Personal Data at the end of the service. These weaknesses are compounded when Personal Data is transferred outside the DIFC to providers abroad without adequacy assessments or standard contractual clauses in place.

12. Legal files may contain criminal records and travel documents may reveal racial or ethnic origin – both types of data would be categorized as Special Categories of Personal Data.
13. As defined in the Comparison Table attached as Annexure 1.

"Sensitive records are also commonly stored in shared drives with broad access and limited security controls, increasing the risk of inappropriate access or loss"

Case Study 2 - Best Practice Approach

To address these gaps, the SFO should:

i. **Appointment of a DPO.**
ii. **Conduct and document a DPIA** before undertaking high-risk activities, such as large-scale handling of Special Categories of Personal Data.
iii. **Maintain a ROPA.**
iv. Engage all vendors under formal **Data Processing Agreements**.
v. **Ensure appropriate controls on cross-border transfers.**
vi. **Ensure a lawful basis** is identified and documented for all Processing activities **and in particular fo the Processing of Special Categories** of Personal Data.
vii. **Provide privacy notices to Data Subjects** to explain why Personal Data is collected, how it will be used, and with whom it will be shared.
viii. **Ensure security limitations are implemented on shared drives to avoid** inappropriate access or loss.
ix. **Implement a formal incident response plan** to detect, investigate, and report any Personal Data breaches.
x. **Ensure that mandatory filings with the data protection regulators are completed** and kept up to date. This includes notifying the DIFC Commissioner when prompted post-incorporation.

"Lack of oversight not only heightens the risk of data loss or misuse but also shift liability back onto the entity itself, which remains responsible for demonstrating compliance under the ADGM DP Regulations and DIFC DP Law."

THIRD-PARTY RISKS AND EXPOSURE

Oversight of third parties is a common compliance gap. Lack of oversight not only heightens the risk of data loss or misuse but also shift liability back onto the entity itself, which remains responsible for demonstrating compliance under the ADGM DP Regulations and DIFC DP Law.

To reduce exposure from vendors and service providers, companies should:

1. **Implement robust Data Processing Agreements (DPAs)** – ensure all vendors sign DIFC/ADGM-compliant contracts covering security, sub-Processing, breach timelines, data return/deletion, and audit rights.
2. **Conduct vendor due diligence** – assess providers before onboarding; request evidence of security certifications and document checks for audit defense.
3. **Implement cross-border safeguards** – map where data travels; if sent outside DIFC/ADGM, require appropriate safeguards (e. g. standard contractual clauses or binding corporate rules) or an adequacy decision issued by the relevant Commissioner.
4. **Ensure ongoing oversight** – don't stop at onboarding; conduct annual reviews, refresh contracts, and test incident escalation to ensure compliance remains current.

PENALTIES

In the DIFC, the Commissioner of Data Protection may impose fines of up to USD 25,000 for failure to notify or update a data Processing registration, and up to USD 100,000 for ongoing or serious violations of the law.[14] Sanctions are published on the DIFC public register, reinforcing reputational consequences alongside financial ones.

In the ADGM, the Office of Data Protection is authorised to impose financial penalties of up to USD 28 million for serious or systemic non-compliance.[15] Penalties are determined in proportion to the scale of the breach, the sensitivity of the data involved, and whether appropriate governance measures were in place.

Both regulators have signalled an **increasing focus on active enforcement**. This includes random audits, formal investigations following complaints, and cooperation with financial and commercial regulators where breaches overlap with other legal duties. Public guidance issued by both the DIFC and ADGM data protection offices has emphasised that accountability is not limited to regulated entities, nor excused by low operational activity.

These obligations apply regardless of whether the entity is licensed or revenue-generating. The "silent stakeholder", Personal Data, demands governance wherever it is collected, used, or stored. Non-compliance is not a theoretical risk. It is a legal exposure that can attract scrutiny and sanctions.

14. DIFC DP Law, schedule 2.
15. ADGM DP Regulations, section 55.

"Data protection compliance in ADGM and DIFC is not only a regulatory obligation but also a matter of good governance. "

CONCLUSION

Data protection compliance in ADGM and DIFC is not only a regulatory obligation but also a matter of good governance. Both frameworks impose duties that extend beyond licensed financial institutions and apply equally to family offices, SPVs, and other private structures. **Failing to put the right safeguards in place can result in penalties, reputational damage, and a loss of trust among stakeholders**. At the same time, robust policies and well-drafted contracts reduce exposure, provide clarity, and allow entities to demonstrate accountability to regulators.

KEY TAKEAWAYS

- Personal data is always present. Treat it as a stakeholder.
- Registration is mandatory. Renewal is ongoing. Compliance is not a tick box exercise.
- Passive or private structures must still comply.
- Compliance obligations are proportionate to activities.

"Robust policies and well-drafted contracts reduce exposure, provide clarity, and allow entities to demonstrate accountability to regulators"

PRACTICAL COMPLIANCE STEPS FOR PRIVATE ENTITIES

- Always ensure **initial notification** and **annual disclosure** is completed.
- **Limit access to Personal Data** strictly to those with a genuine business need, supported by role-based permissions and audit trails.
- **Map and document what Personal Data you hold**, why you hold it, and who has access to it, as would be detailed in:
  - a ROPA,
  - an internal directive; and/or
  - clear privacy notices shared with Data Subjects (e.g. for shareholders, directors, or employees).
- **Put data processing agreements in place** with service providers, advisers, and IT vendors.
- **Review cross-border transfers** and identify whether appropriate safeguards are required depending on an adequate jurisdiction finding.
- **Set retention rules** so data is deleted, anonymised, or put beyond use when no longer required.
- **Establish a breach response plan** and train staff on when and how to send a notification.
- **Assess the need for a DPO or DPIA** where large-scale, sensitive, or high-risk Processing occurs.

ABOUT THE AUTHORS

Hermione Harrison
Partner and Senior Director
M/HQ
harrison@m-hq.com

Gina Omer
Associate
lecocqassociate
lom@lecocqassociate.com

Hermione Harrison is Partner and Senior Director at M/HQ and leads the Abu Dhabi office. She was admitted as a solicitor of the Supreme Court of New South Wales, Australia. She holds an LLB (Hons) and a BA in Political Science. She is a senior adviser with more than 18 years of international legal and governance experience across Asia, Europe, Africa and the Middle East.

At M/HQ Hermione leads advisory work on corporate governance, international wealth structuring and compliance for private clients, family offices and cross border enterprises. She advises on ADGM and DIFC foundations and family office structures with a focus on succession planning and ongoing compliance. She works closely with UAE regulators and contributes to regional policy and thought leadership.

Gina Omer is a U.S.-qualified corporate and commercial lawyer based in the United Arab Emirates. As an Associate at lecocqassociate, she advises financial institutions, fund managers, and businesses on cross-border structuring, investment fund formation, mergers and acquisitions, shareholder arrangements, and corporate governance matters. Her practice also covers data protection compliance, financial services regulation, and the negotiation of complex service-provider agreements, with a particular focus on aligning UAE structures with international best practices. She regularly contributes to thought leadership on regulatory and data protection matters in the UAE.

M/HQ is a multi-services platform catering to financial institutions as well as single family offices and sophisticated private investment companies. Our one-stop-shop offering is unique in the Middle East: a holistic and cross-disciplinary blend of a leading corporate services firm, private client specialist team, and a regulatory & compliance services practice, all through one single platform.

We have extensive experience advising on a broad range of wealth structuring and legacy planning issues. We particularly assist in establishing and servicing family- and group- holdings, single- and multi- family offices, foundations, and other asset consolidation/ protection and intergenerational wealth management structures. For financial institutions, we provide tailored solutions that address complex regulatory and compliance requirements, ensuring that operations are both secure and efficient.

Headquartered in the UAE, we are an entrepreneurial firm for entrepreneurial clients.

lecocqassociate is an international boutique law firm and regulatory advisory practice with offices in Geneva, Malta, Dubai (DIFC), and Abu Dhabi (ADGM). With over 40 professionals, we combine global insight with local knowledge to deliver innovative, practical solutions in regulatory finance, corporate and commercial law, private equity, M&A, and data protection. Our hands-on, client-focused approach helps financial institutions, fund managers, and entrepreneurs navigate complex cross-border transactions and regulatory landscapes with clarity and confidence.

ADGM AND DIFC DATA PROTECTION COMPARISON TABLE

Key Definitions *(Please note that the below terms are defined in a general manner to accommodate both the ADGM DP Regulations and the DIFC DP Law, rather than replicating the exact wording of the defined terms in each jurisdiction.)*	
Controller	means a person who, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
Data Subject	means an identified or identifiable natural person to whom Personal Data relates.
Personal Data	means any information relating to an identifiable natural person.
Processing	means any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission or otherwise making available, alignment or combination, restriction, erasure or destruction.
Processor	means a person who Processes Personal Data on behalf of a Controller.
Special Categories of Personal Data	means Personal Data revealing or concerning racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, trade-union membership, sex life- health, genetic or biometric data (where used for identification purposes), and criminal records.

TOPIC	ADGM	DIFC	KEY TAKEAWAYS
Scope – Material and Territorial	Both jurisdictions apply to the Processing of Personal Data by a Controller or Processor that is established in each jurisdiction, regardless of where the Processing takes place, however each jurisdiction includes a different element of extraterritorial reach.		In the ADGM, where a Processor is Processing Personal Data for a Controller outside the ADGM, the Processor must comply with the requirements of the ADGM DP Regulations to the extent possible, taking into account whether the Controller is subject to similar obligations under the laws of its home jurisdiction.

			In the DIFC, the DIFC DP Law applies to the Processing of a Personal Data by a Controller or Processor, regardless of its place of incorporation as part of stable arrangements, including transfers of Personal Data out of the DIFC.
Core Principles	Both jurisdictions have similar core principles when Processing Personal Data such as the following: i. **Lawful & Fair** – Processed only on a valid legal basis (as practically applied in the case studies below) and handled fairly and transparently with respect to the Data Subject. ii. **Purpose-Specific** – Collected for specified, explicit, and legitimate purposes and not used for incompatible purposes later. iii. **Data Minimisation** – Limited to what is relevant, adequate, and necessary for the stated purpose. iv. **Respectful of Data Subject Rights** – Processed in a way that enables and supports the exercise of Data Subject rights under the law. v. **Accurate & Up to Date** – Kept accurate and, where needed, corrected or erased without undue delay. vi. **Retention-Limited** – Retained only as long as necessary for the purposes for which it was collected. vii. **Secure** – Protected against unauthorised or unlawful access, transfers, loss, destruction, or damage through appropriate technical and organisational measures.		
Special Categories of Personal Data	Both jurisdictions prohibit Processing of Special Categories of Personal Data unless a specific condition is met including but not limited to (i) the Data Subject gave their explicit consent; (ii) Processing is necessary to carry out employment-related obligations; or (iii) processing is necessary to comply with applicable law that applies to a Controller in relation to anti-money laundering or counter-terrorist financing obligations or the prevention, detection or prosecution of any crime.		It is worth noting that the ADGM DP Regulations also allow Processing Special Categories of Personal Data for the performance of a contract to which the Data Subject is party to.

Consent	In both jurisdictions, consent must be a clear, specific, informed, and unambiguous indication of a Data Subject's wishes, expressed through a positive action (not silence or pre-ticked boxes). It must be freely given, distinguishable from other matters, and based on clear and plain language. Where relied upon, consent constitutes a lawful basis of Processing, and Controllers must be able to demonstrate its validity, inform Data Subjects of their right to withdraw at any time, and ensure that withdrawal is as easy as giving consent.	The DIFC lays out a detailed framework for ongoing consent management: it requires periodic reassessment and re-affirmation of consent unless the Processing relates to a one-off, non-recurring transaction or a clearly defined, time-limited purpose. DIFC also mandates procedures for recording and evaluating consent and sets expectations around contacting Data Subjects if continued Processing is no longer reasonably expected.
Data Subject Rights	Both jurisdictions provide comparable rights to Data Subjects, namely (i) the right of access to Personal Data that is processed; (ii) the right to rectification of inaccurate or incomplete Personal Data; (iii) the right to erasure ("right to be forgotten"); (iv) the right to restrict Processing; (v) the right to data portability; (vi) the right to object to Processing, including for direct marketing; (vii) the right not to be subject to decisions based solely on automated Processing, including profiling, which produce legal or similarly significant effects; (viii) the right to withdraw consent at any time; and (ix) the right to lodge a complaint with the relevant Commissioner of data protection.	

Record of Processing (ROPA)	Required to be in place for both Controllers and Processors	Required to be in place for both Controllers and Processors, however there is a relief for smaller entities with less than 50 staff members, unless the Processing is high-risk	A ROPA is required in the ADGM regardless of company size. However, in the DIFC, there is an exemption for smaller entities unless conducting high risk Processing activities such as Processing with new technology methods that pose an increased security risk to the Data Subject.
Appointment of Data Protection Officer	Only required to be appointed if the Processing is conducted by a public authority, or if the core activities of a Controller or Processor consists of Processing on a large-scale. Such DPO can be external and may be based outside of ADGM.	Only required if the Processing is conducted by a public authority, or if performing high-risk Processing[16] activities on a regular basis. Such DPO must be based in the UAE, unless a group-wide DPO is appointed and performs a similar function on an international basis.	In the event a DPO is not appointed, a Controller or Processor must clearly allocate the responsibility for data protection oversight and compliance with the relevant legislation. The key point being the DPO or responsible individual must be easily accessible for the relevant entity.
Annual Processing Assessment	Not mandated by law	Required to be submitted annually in the event a DPO is appointed.	The DIFC DP Law imposes a recurring requirement where a DPO is appointed.

16. A few examples of high risk processing activities may include adoption of new technologies, processing a considerable amount of Personal Data where it is likely to risk the integrity and privacy of such data, or a considerable amount of Special Categories of Personal Data.

Data Protection Impact Assessment ("DPIA")	In both jurisdictions, DPIA must be carried out before undertaking Processing that is likely to result in a high risk to the rights of individuals[17]. A single DPIA can cover similar Processing operations, must describe the proposed activities and their purposes, assess necessity and proportionality, identify risks to Data Subjects, and set out measures to mitigate those risks. Both frameworks require the involvement of a Data Protection Officer (where appointed) and mandate reviews when risks or circumstances change, ensuring that Processing remains aligned with the DPIA. Both jurisdictions require a notice to the Commissioner where a DPIA shows high risk.	The DIFC DP Law permits reliance on a DPIA already carried out by another entity within the same corporate group, provided it remains current and accurate.
Reporting Data Breaches	Both jurisdictions require entities to notify the respective Commissioner as soon as reasonably practicable in the event of a Personal Data breach—within 72 hours in the case of ADGM—and to notify affected Data Subjects where the breach is likely to result in a high risk of harm. Where individual notifications would involve a disproportionate effort, both regimes permit a public or mass communication method to ensure Data Subjects are informed.	
International Transfers	A transfer of Personal Data outside of either jurisdiction may only take place where: (i) the recipient jurisdiction has been formally deemed by the relevant Commissioner to provide an adequate level of data protection, or (ii) the Controller or Processor in question has provided appropriate safeguards. A few examples of appropriate safeguards include, but are not limited to, the relevant entity having binding corporate rules or implementing standard data protection clauses[18].	
Cessation of Processing	In both jurisdictions, Personal Data must not be retained once Processing is no longer necessary, and must either be deleted, anonymised, or otherwise put beyond use, subject to limited exceptions such as legal obligations, compliance, or certain public-interest purposes.	

17. Please see Footnote 16 on examples of high risk processing activities.
18. These clauses can typically be found in your data transfer agreements between Controller and Processor, and the Office of Data Protection in each of the ADGM and DIFC have posted model clauses to be used in data transfer agreements.