ICLG

The International Comparative Legal Guide to:

Data Protection 2016

3rd Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Affärsadvokaterna i Sverige AB
Bagus Enrico & Partners
Cuatrecasas, Gonçalves Pereira
Deloitte Albania Sh.p.k.
Dittmar & Indrenius
ECIJA ABOGADOS
Eversheds SA
Gilbert + Tobin
GRATA International Law Firm
Hamdan AlShamsi Lawyers & Legal Consultants
Herbst Kinsky Rechtsanwälte GmbH
Hogan Lovells BSTL, S.C.
Hunton & Williams
Lee and Li, Attorneys-at-Law
Matheson
Mori Hamada & Matsumoto
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi
Rossi Asociados
Subramaniam & Associates (SNA)
Wigley & Company
Wikborg, Rein & Co. Advokatfirma DA

global legal group

global legal group

Contributing Editor
Bridget Treacy,
Hunton & Williams

Sales Director
Florjan Osmani

Account Directors
Oliver Smith, Rory Smith

Sales Support Manager
Toni Hayward

Sub Editor
Hannah Yip

Senior Editor
Rachel Williams

Chief Operating Officer
Dror Levy

Group Consulting Editor
Alan Falach

Group Publisher
Richard Firth

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd.
April 2016

ISBN 978-1-910083-93-2
ISSN 2054-3786

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

General Chapter:

Country Question and Answer Chapters:

United Arab Emirates

Hamdan AlShamsi Lawyers & Legal Consultants

Dr. Ghandy Abuhawash

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The UAE has not established a specific federal data protection law, although certain federal laws recognise an individual right to privacy as well as confidential information regarding companies and employees. Such federal laws include criminal, civil, commercial, and labour provisions. In the Dubai International Finance Centre (DIFC) data protection laws and regulations have been enacted and are closely based upon the UK's data protection law.

1.2 Is there any other general legislation that impacts data protection?

The DIFC has its own data protection specific laws and regulations; however, these laws are only applicable to activities within the DIFC. The laws apply to specific types of personal information which is related to certain individuals, and the law sets out obligations to ensure personal data is processed in a fair, lawful, legitimate and secure way.

1.3 Is there any sector specific legislation that impacts data protection?

Yes, the following are sectoral laws:

- **The Penal Code**: Federal Law No. 3 of 1987 deals with criminal provisions to protect the use of personal data. The law protects the usage of personal and confidential data of persons, as well as the leakage of personal and corporate data.
- **Cybercrime**: Federal Law No. 5 of 2012 deals with combatting cybercrime activities, such as hacking, identity theft and fraud. The law also regulates unauthorised access of websites or electronic information systems and networks, as well as imposing penalties for the republication of data. Furthermore, the law prohibits invasion of privacy of an individual through a computer network and the disclosure of confidential information.
- **Telecommunications**: Federal Law No. 3 of 2003 applies to data which is obtained through any means of telecommunications, and which is regulated by the Telecommunications Regulatory Authority (TRA).
- **Privacy of Consumer Information Policy**: The policy applies to entities that have access to personal information. This also applies to all telecommunications.
- **Dubai Statistics Centre**: Dubai Law No. 23 of 2006 relates to the specific collection and publication of data in the Emirate of Dubai only. The law restricts the disclosure of personal data and information obtained through statistical collection.
- **DIFC**: Data Protection Law Amendment Law, DIFC Law No. 5 of 2012 and Data Protection Regulations Consolidated Version No. 2 of 2012. The DIFC legislation is mainly consistent with data protection laws of the European Union and UK common law.
- **Dubai Healthcare City (DHCC)**: Federal Law No. 10 of 2008. The law is concerned with medical liability as well as patient confidentiality.

1.4 What is the relevant data protection regulatory authority(ies)?

The UAE has no single authority regulating data protection, but rather a collection of sectoral authorities:

- UAE Telecommunications Regulatory Authority (TRA).
- DIFC Commissioner of Data Protection.
- Dubai Healthcare City, Centre for Healthcare Planning and Quality.
- Ministry of Justice.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- **"Personal Data"**

  Personal data is not defined in UAE law; there is only reference to a general right to privacy for citizens defined in the constitution. Additionally, the Penal Code of the UAE provides that the publication of any personal data which relates to an individual's private or family life is an offence. The DIFC Law defines personal data as "any data referring to an identifiable natural person".

- **"Sensitive Personal Data"**

  There is no definition for sensitive personal data or other types of personal data, although the Cybercrime Law does impose more severe penalties in instances where unauthorised actions relate to personal data. The DIFC defines sensitive personal data as "personal data revealing or concerning racial or ethnic origin, communal origin, political affiliation or opinions, religious or philosophical beliefs, criminal record, trade union membership and health or sex life".

- **"Processing"**

  There are no obligations under UAE law if data is processed properly. However, the Cybercrime Law and Privacy of Consumer Information Policy do require service providers to take adequate measures protecting unauthorised use or disclosure of personal data. The DIFC Law defines processing as any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage and others.

  There is also processing for consent of use of personal data and processing by third parties of data.

- **"Data Controller"**

  Since the UAE does not have a specific data protection law, it does not recognise such concepts as data processors and controllers. The DIFC Law defines data controllers as "any person in the DIFC who alone or jointly with others determines the purposes and means of the processing of personal data".

- **"Data Processor"**

  Since the UAE does not have a specific data protection law, it does not recognise such concepts as data processors and controllers. The DIFC Law defines a data processor as anyone acting under a data controller and who has access to confidential information.

- **"Data Subject"**

  A data subject is not defined but it is implied that this is a person. Consent is required from a data subject to process personal data; there are no rules on the form of consent, as it can be implied or inferred. The DIFC defines the data subject as "the individual to whom the personal data relates".

- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*

  The following are mentioned and defined in the Cybercrime Law:

  - **"Electronic Information"**

    Any information which is stored, processed, generated, transmitted through information technology systems and in specific writings, images, sound, digits, letters, symbols, signals, and others.

  - **"Government Data"**

    Electronic data or information, whether private or relating to the federal government or local governments of the Emirates of the state, or to federal or local public authorities or public establishments.

  - **"Confidential"**

    Any information or data unauthorised to be disclosed or made available to third parties unless by prior permission from the owner of this authorisation.

3 Key Principles

3.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

  There are general regulations on the processing of personal data stipulated in the DIFC Law for data protection. Transparency processing must be "specified, explicit, and for legitimate purposes in accordance with the data subject's rights".

- **Lawful basis for processing**

  All data must be processed "fairly, lawfully and securely"; immigration and national security bodies may process data in the interest of national security.

- **Purpose limitation**

  Data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes of which the personal data was collected.

- **Data minimisation**

  Data will only be processed if the data subject has given his written consent to the processing of that personal data. Only necessary data shall be processed.

- **Proportionality**

  Data must be adequate, relevant and not excessive in relation to purposes for which it is collected and/or further processed.

- **Retention**

  Every reasonable step is taken by data controllers to ensure that personal data which is inaccurate or incomplete is erased or rectified.

- *Other key principles – please specify*

  There are also other requirements for the processing of sensitive personal data in the DIFC Law, in addition to the transfer of data outside the DIFC.

4 Individual Rights

4.1 What are the key rights that individuals have in relation to the processing of their personal data?

The following answers will be in reference to DIFC Data Protection Law.

- **Access to data**

  An individual has the right to access his data from the data controller upon a request. Confirmation in writing may be accessed regarding whether or not personal data relating to him is being processed, as well as the reasons why his information is being processed.

- **Correction and deletion**

  If the data does not comply with the provisions of the law, then data may be rectified or deleted.

- **Objection to processing**

  An individual has the right to object at any time on reasonable grounds.

- **Objection to marketing**

  An individual has the right to be informed before his data is disclosed for the first time to a third party, as well as when it is to be used on their behalf for the purposes of direct marketing.

- **Complaint to relevant data protection authority(ies)**

  Complaints are heard and filed in front of the Commissioner of Data Protection.

- *Other key rights – please specify*

  There are no other key rights in particular.

5 Registration Formalities and Prior Approval

5.1 In what circumstances is registration or notification required to the relevant data protection regulatory authority(ies)? (E.g., general notification requirement, notification required for specific processing activities.)

A data controller must notify the Commissioner of Data Protection regarding personal data processing operations such as a set of operations involving the processing of personal and sensitive data, or any personal data processing operations involving the transfer of personal data to an individual outside the DIFC.

There are different types of reasons to make notifications under federal law. These could be for notification of gathering public data for the purpose of statistics.

5.2 On what basis are registrations/notifications made? (E.g., per legal entity, per processing purpose, per data category, per system or database.)

Notifications are made on the basis of situations regarding the records of personal data administered by the data controllers and on the grounds provided in question 5.1.

5.3 Who must register with/notify the relevant data protection authority(ies)? (E.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation.)

The data controller shall make a registration or notification to the Commissioner of Data Protection. The DIFCA Board of Directors shall then make regulations after consulting with the Commissioner.

5.4 What information must be included in the registration/notification? (E.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes.)

A notification must contain the following information:

- a general description of the personal data processing being carried out;
- an explanation of the purpose for the personal data processing;
- the data subjects or class of data subjects whose personal data is being processed;
- a description of the class of personal data being processed; and
- a statement of which jurisdictions to which personal data will be transferred by the data controller, along with an indication as to whether the particular jurisdiction has been assessed as having adequate level of protection.

5.5 What are the sanctions for failure to register/notify where required?

Administrative fines may be imposed on data controllers; the fine will not be recovered as a debt due, but the Commissioner may instead commence proceedings in the court for payment of the fine.

Sanctions on the federal law side take into account the purpose of failure to notify, the affect the failure had on the person, and moral or tangible aspects. There are various sanctions that can be made, which are either criminal penalties, and/or administrative fines.

5.6 What is the fee per registration (if applicable)?

There are three categories for registration: category one costs $1,000; category two costs $500; and category three costs $200.

5.7 How frequently must registrations/notifications be renewed (if applicable)?

Registration is renewed annually.

5.8 For what types of processing activities is prior approval required from the data protection regulator?

The following processing activities require prior approval:

- processing personal sensitive data; and
- transfer of personal data out of DIFC.

5.9 Describe the procedure for obtaining prior approval, and the applicable timeframe.

An application must be made to the Commissioner in writing to acquire a permit. The application requires various supporting documents describing what is needed. Upon permission, a fee is paid depending on the processing activity and category.

6 Appointment of a Data Protection Officer

6.1 Is the appointment of a Data Protection Officer mandatory or optional?

In the DIFC Data Protection Law, the Data Protection Officer is referred to as the Commissioner of Data Protection. The President of Data Protection shall appoint the Commissioner of Data Protection.

6.2 What are the sanctions for failing to appoint a mandatory Data Protection Officer where required?

There are no sanctions for failing to appoint the Commissioner of Data Protection. The Commissioner is appointed by the President for a period of three years, at which the Commissioner may resign at any point, providing three months' notice.

6.3 What are the advantages of voluntarily appointing a Data Protection Officer (if applicable)?

The Commissioner may delegate powers as he sees fit to other officers or employees.

6.4 Please describe any specific qualifications for the Data Protection Officer required by law.

The Commissioner is appointed at the discretion of the President; the law dictates that the President must choose a Commissioner who is appropriately experienced and qualified.

6.5 What are the responsibilities of the Data Protection Officer, as required by law or typical in practice?

The main function of the Commissioner is to exercise his powers in accordance with the law. The Commissioner's objective is to promote good practices and observance of requirements of the law and regulations, while also promoting awareness and public understanding of data protection.

6.6 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

The appointment of the Commissioner is consulted with the DIFC Board of Directors.

7 Marketing and Cookies

7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, email, or SMS text message. (E.g., requirement to obtain prior opt-in consent or to provide a simple and free means of opt-out.)

An individual may object to the use of his personal data when it is used for the purpose of direct marketing.

Consent is required when sending marketing SMS text messages. For new mobile customers, an opt-in consent request is sent, and for existing mobile users who wish to withdraw their consent, an opt-out option is available.

7.2 Is the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The TRA is the authoritative body in charge of enforcing marketing restrictions. A regulatory policy was issued in 2009: the Unsolicited Electronic Communications Policy. The policy provides that there is an obligation put in place to minimise the transmission of spam and marketing telecommunications sent without consent.

7.3 Are companies required to screen against any "do not contact" list or registry?

Generally, this is not a common practice in the UAE.

7.4 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

A telecommunications provider who breaches the TRA regulations will have appropriate penalties enforced against him at the discretion of the authority.

7.5 What types of cookies require explicit opt-in consent, as mandated by law or binding guidance issued by the relevant data protection authority(ies)?

All types of cookies are used on websites in the UAE; however, there is no provision in the law stating which websites must notify using an explicit opt-in consent.

7.6 For what types of cookies is implied consent acceptable, under relevant national legislation or binding guidance issued by the relevant data protection authority(ies)?

The law does not reference on the requirement of implied or explicit consent through websites in the UAE.

7.7 To date, has the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

No, action is mainly against marketing purposes and third party users.

7.8 What are the maximum penalties for breaches of applicable cookie restrictions?

To date, there is no maximum penalty for breaches of applicable cookie restrictions.

8 Restrictions on International Data Transfers

8.1 Please describe any restrictions on the transfer of personal data abroad?

The Penal Code requires data subjects to provide consent for the transfer of personal data inside or outside the UAE.

The DIFC Law allows for the process of international data transfer only if there is adequate protection for that data ensured by the law and regulations. A safe jurisdiction in which to transfer data is listed under the Data Protection Regulations. In the absence of adequate protection, the Commissioner may give written authorisation if the conditions of that transfer are satisfied.

8.1 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions.

Data is transferred though data controllers and processors, who must abide by federal and DIFC Law and regulations.

8.2 Do transfers of personal data abroad require registration/notification or prior approval from the relevant data protection authority(ies)? Describe which mechanisms require approval or notification, what those steps involve, and how long they take.

Transfer of data which do not have adequate protection under the DIFC Law must satisfy certain conditions such as: the data subject has given his consent; the transfer is necessary for the performance or conclusion of a contract; the transfer is necessary to protect vital interests of data; and others.

9 Whistle-blower Hotlines

9.1 What is the permitted scope of corporate whistle-blower hotlines under applicable law or binding guidance issued by the relevant data protection authority(ies)? (E.g., restrictions on the scope of issues that may be reported, the persons who may submit a report, the persons whom a report may concern.)

There are no whistle-blower hotlines in the UAE. The UAE is a party to the UN Anti-Corruption Convention; however, there is no specific law relating to the regulation of whistle-blowing. Generally, various international and multinational companies in the UAE develop their own internal procedures to adopt requirements.

9.2 Is anonymous reporting strictly prohibited, or strongly discouraged, under applicable law or binding guidance issued by the relevant data protection authority(ies)? If so, how do companies typically address this issue?

The Abu Dhabi Accountability Authority has developed an anti-fraud and anti-corruption framework to assist state-owned companies and government entities. There are no provisions in the law against reporting, nor is it common practice to discourage employees from doing so.

9.3 Do corporate whistle-blower hotlines require separate registration/notification or prior approval from the relevant data protection authority(ies)? Please explain the process, how long it typically takes, and any available exemptions.

No, the data protection authorities in the UAE do not make reference to procedures concerning whistle-blowing or reporting.

9.4 Do corporate whistle-blower hotlines require a separate privacy notice?

Some companies issue an internal whistle-blower policy; however, this does not enable protection. The only provision in the law giving implied protection is in the UAE Labour Law.

9.5 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

Employees are notified of whistle-blowing policies internally. The only protection that is offered in the Labour Law is where an employee is dismissed for having "submitted a serious complaint to the competent authorities"; this will be arbitrary.

10 CCTV and Employee Monitoring

10.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies)?

In Dubai, the use of CCTV cameras is regulated by Dubai Law No. 10 of 2014. The law makes the installation of CCTV cameras compulsory for all buildings in Dubai. Moreover, there are fines for not complying with this law.

10.2 What types of employee monitoring are permitted (if any), and in what circumstances?

The following types of employee monitoring are permitted in the UAE:

- employee property, such as desktops, computers, laptops, etc.; and
- keystrokes, email content, and screens.

10.3 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Consent must be obtained from the employees under the Cybercrime Law and Telecommunications Law. Without consent, monitoring is prohibited, especially if the data monitored is sensitive, such as private and family life. Clear monitoring policies in workplaces are sometimes suggested to clarify monitoring procedures of a company.

10.4 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

UAE law does not conduct such procedures, and only the DIFC Law provides notification provisions.

10.5 Does employee monitoring require separate registration/notification or prior approval from the relevant data protection authority(ies)?

Since there is no single data protection authority in the UAE, there is no process of prior approval or notification. Only in the DIFC do such procedures apply.

11 Processing Data in the Cloud

11.1 Is it permitted to process personal data in the cloud? If so, what specific due diligence must be performed, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

When signing in with a cloud provider, a user may be private or public, or a hybrid user. Personal data may be processed on the cloud, and in particular, a user must be careful not to process any personal data without consent, or they will fall subject to the Penal Code prohibition on the disclosure of secrets. There are data centres within the UAE that usually support this service, the main providers being Etisalat and Du.

11.2 What specific contractual obligations must be imposed on a processor providing cloud-based services, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Rules governing document retention are important to note. The Commercial Transactions Law sets out general requirements for the retention of commercial records. Company records on the cloud must be stored only for a minimum of five years to comply

with the Law. General contractual obligations are imposed on a cloud provider; the main one being on sharing data with third-parties. Most Dubai-based data centres do not resell third party core infrastructures.

12 Big Data and Analytics

12.1 Is the utilisation of big data and analytics permitted? If so, what due diligence is required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Yes, big data and analytics is widely utilised in the UAE to collect statistics in several sectors. Data collection in Dubai is regulated by the Dubai Statistics Centre, where statistical findings are sometimes published in reports.

13 Data Security and Data Breach

13.1 What data security standards (e.g., encryption) are required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Data security is provided in the Penal Code and Cybercrime Law. There are several penalties for breaching the data security standards.

13.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

No, there is no legal requirement enforcing the reportage of data breaches.

13.3 Is there a legal requirement to report data breaches to individuals? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

The position is the same for reporting data breaches to individuals; there is no enforcement rule.

13.4 What are the maximum penalties for security breaches?

Under the Cybercrime Law, a breach of security through a website shall be punishable by temporary imprisonment and a fine which does not exceed one million dirhams. Other offences also amount to a security breach and are all punishable with imprisonment. Some of these include: accessing a website to obtain government data without authorisation; running a website that promotes ideas of racism, hatred, sectarianism, and ideas against the public order of the UAE; running a website on behalf of a terrorist group; and publishing information that is incorrect and misleading which may damage the interests of the state and disclose an entrusted secret.

14 Enforcement and Sanctions

14.1 Describe the enforcement powers of the data protection authority(ies):

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
UAE Telecommunications Regulatory Authority (TRA)	■ Suspend an operator's licence if the licensee is in breach of the licence conditions. ■ Compliance with all directions from the Authority on matters relating to public interest, safety and national security.	■ Licensee suspension in the interest of national security with imprisonment, in accordance with the Penal Code and Cybercrime Law. ■ The use of encryption techniques may lead to imprisonment, in accordance with the Penal Code and Cybercrime Law.
DIFC Commissioner of Data Protection	■ Entities must notify the Authority to process personal data. ■ Transferral of data outside of the DIFC should be gained through a permit in the Authority. ■ Permit to process sensitive personal data must be gained through the Authority. ■ Records must be kept in relation to personal data processing. ■ An administrative fine may be imposed by the Authority for contravention of the DIFC data regulations; failure to pay the fine shall result in civil proceedings in the courts.	■ Court proceedings when an entity has been in direct breach of the DIFC Data Protection Law and regulations. ■ Criminal fines may be imposed when a contravention with the law has occurred.
Dubai Healthcare City, Centre for Healthcare Planning and Quality	■ The Authority may audit a licensee for assurance that the treatment of patient health data is handled in compliance with the DHCC data regulations. ■ Restrictions issued by the Authority on the disclosure of patient health records and identification information are imposed. Failure to comply results in administrative discipline.	■ Criminal penalties may be initiated when there is a direct breach of the DHCC regulations and the nature of the breach would need to refer to Penal Code.

14.2 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

1. Case No. 175/2001: this case involved a leak of personal data, which is an offence under the Penal Code.
2. Case No. 43/2005: it is an offence to leak information for your own benefit under article 379 of the Penal Code.
3. Case No. 146/2004: there are certain conditions that constitute an offence to leak confidential information (such as the nature of the data leaked, the moral and tangible details of the secret, whether the secret was used for personal benefit or for the benefit of others, etc.).

Data protection in the UAE is still very much a fresh concept, and most of the cases decided are regarding a leak of company data rather than personal.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

15.1 How do companies within your jurisdiction respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Discovery requests fall under the Evidence Law of the UAE; requests for discovery and disclosure may be enforced in litigation proceedings. However, e-discovery requests are conducted in line with the federal data protection provisions.

15.2 What guidance has the data protection authority(ies) issued?

The data protection authorities in the UAE do not provide guidance on disclosure. Disclosure of documents is only referred to in the Penal Code and Cybercrime Law as a type of breach, in addition to the Evidence Law as mentioned above.

16 Trends and Developments

16.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

The medical liability law was established in 2008 and this was an important piece of legislation to protect the confidential information of patients. The DIFC Data Protection Law was also amended to include penalties for various provisions of the legislation.

16.2 What "hot topics" are currently a focus for the data protection regulator?

There are various initiatives in the UAE to improve data protection. There are even talks of provisions in the law being amended to be based on EU Data protection laws, but this remains to be seen. Whistle-blower legislation has also been discussed, but so far, only Abu Dhabi has initiated whistler-blower protections for governmental entities.

Dr. Ghandy Abuhawash
Hamdan AlShamsi Lawyers &
Legal Consultants
Office 1611, 16th Floor, Al Manara Tower
Al Abraj Street
Business Bay, Dubai
United Arab Emirates

Tel: +971 4 3469262
Email: ghandy@alshamsilegal.com
URL: www.alshamsilegal.com

Dr. Ghandy Abuhawash has over 15 years of experience in legal services. He has represented clients in both contentious and non-contentious matters. Dr. Ghandy Abuhawash specialises in company law, advising on shareholder agreements, compliance issues, labour law, intellectual property law, criminal disputes, commercial disputes and corporate matters. In addition to private and in-house practice, Dr. Ghandy Abuhawash is a leading arbitrator and has handled various high-profile cases within the UAE and abroad. Moreover, Dr. Ghandy Abuhawash is an accomplished academic and holds a Ph.D. in Law and Legal Studies, as well as a published thesis.

HAMDAN ALSHAMSI
LAWYERS & LEGAL CONSULTANTS

Hamdan AlShamsi Lawyers & Legal Consultants was established in 2011. It has since become a name synonymous with success and is well-known in the legal circuit. The success of the law firm is due to its specialisation in advising on commercial issues, insurance, due diligence, family law, intellectual property law, banking, companies law and other matters locally, and its dedication towards offering unparalleled, high-quality and culturally sensitive legal services, while adhering to the highest standards of integrity and excellence.

Other titles in the ICLG series include:

- Alternative Investment Funds
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Recovery & Insolvency
- Corporate Tax
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: sales@glgroup.co.uk

www.iclg.co.uk