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:

South Africa

Eversheds SA

Tanya Waksman

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The Protection of Personal Information Act 4 of 2013 ("**POPI**") is the principal data protection legislation in South Africa.

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

Yes, namely the Consumer Protection Act 68 of 2008, the Electronic Communications and Transactions Act 25 of 2002, the Regulation of the Interception of Communications and Provision of Communication-Related Information Act 70 of 2002, and the Promotion of Access to Information Act 2 of 2000.

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

No, there is no such legislation in South Africa.

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

The Information Regulator, established in terms of section 39 of POPI, and the Enforcement Committee, established in terms of section 50 of POPI.

2 Definitions

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

- **"Personal Information"**

  This means information relating to an identifiable, living, natural person and, where it is applicable, an identifiable, existing juristic person, including, but not limited to:

  (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

  (b) information relating to the education or the medical, financial, criminal or employment history of the person;

  (c) any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

  (d) the biometric information of the person;

  (e) the personal opinions, views or preferences of the person;

  (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

  (g) the views or opinions of another individual about the person; and

  (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

- **"Special Personal Information"**

  This means the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or the alleged criminal behaviour of a data subject.

- **"Processing"**

  This means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

  (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

  (b) dissemination by means of transmission, distribution or making available in any other form; or

  (c) the merging, linking, as well as the restriction, degradation, erasure or destruction of information.

- **"Responsible Party"**

  This means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

- **"Operator"**

  This means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.

- **"Data Subject"**

  This means the person to whom personal information relates.

- **"Record"**

  This means any recorded information:

  (a) regardless of form or medium, including any of the following:

  i. writing on any material;

  ii. information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;

  iii. label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;

  iv. book, map, plan, graph or drawing; or

  v. photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;

  (b) in the possession or under the control of a responsible party;

  (c) whether or not it was created by a responsible party; and

  (d) regardless of when it came into existence.

3 Key Principles

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

- **Accountability**

  The responsible party must ensure that POPI is complied with and that all measures that give effect to such conditions are complied with at the time of the determination of the purpose and means of the processing, and during the processing, of personal information.

- **Processing limitation**

  Personal information must be processed:

  (a) lawfully;

  (b) in a manner that is not excessive in relation to the purpose for which it is processed;

  (c) in a manner that does not infringe the privacy of the data subject; and

  (d) with any of the following:

  i. the consent of the data subject;

  ii. if otherwise justifiable to protect the legitimate interests of the data subject;

  iii. to comply with public law;

  iv. processing complies with an obligation imposed by law; or

  v. if necessary for pursuing the legitimate interests of the responsible party or a third party to whom the information was supplied.

- **Purpose specification**

  Personal information must be collected for a specific, explicitly defined and lawful purpose. The data subject must be made aware of the purpose of collection of the personal information collected. Records of personal information must not be retained any longer than is necessary for achieving the purpose for which the personal information was collected.

- **Further processing limitation**

  Further processing of personal information must be in accordance or compatible with the purpose for which it was collected.

- **Information quality**

  The responsible party must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary.

- **Openness**

  The responsible party must maintain the documentation of all processing operations under its responsibility. The responsible party must take reasonably practicable steps to ensure that the data subject is aware that its personal information is being collected, who is collecting it and for what purpose it is being collected.

- **Security safeguards**

  The responsible party must secure the integrity and confidentiality of personal information in its possession or under its control. In the event of a breach, the responsible party must notify the Information Regulator and the data subject.

- **Data subject participation**

  The data subject must be given access to its personal information and have the ability to correct or delete any error in relation thereto.

4 Individual Rights

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

- **Access to data**

  The data subject has the right to establish whether a responsible party holds personal information of that data subject and to request access to his personal information.

- **Correction and deletion**

  The data subject has the right to request, where necessary, the correction, destruction or deletion of his personal information.

- **Objection to processing**

  The data subject has the right to object, on reasonable grounds, to the processing of his personal information.

- **Objection to marketing**

  The data subject has the right to object to the processing of his personal information for purposes of direct marketing at any time.

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

  The data subject has the right to submit a complaint to the Information Regulator regarding the alleged interference with the protection of the personal information of any data subject, or to submit a complaint to the Information Regulator in respect of a determination of an adjudicator, and to institute civil proceedings regarding the alleged interference with the protection of his personal information.

- **Notification**

  The data subject has the right to be notified that:

  (a) personal information about him is being collected; or

  (b) his personal information has been accessed or acquired by an unauthorised person.

- **Decision-making**

  The data subject has the right not to be subject to a decision based solely on the basis of automated processing of his personal information where such is intended to provide a profile of that person.

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.)

No registration is currently provided for.

Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify the Information Regulator as soon as reasonably possible after the discovery of the compromise.

Prior authorisation of the Information Regulator is also required where the responsible party plans to:

(a) process any unique identifiers of data subjects:
  (i) for a purpose other than the one for which the identifier was specifically intended at collection; and
  (ii) with the aim of linking the information together with information processed by other responsible parties;

(b) process information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties;

(c) process information for the purposes of credit reporting; or

(d) transfer special personal information, or the personal information of children, to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information.

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

See question 5.1 above.

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.)

Any responsible party seeking to process personal information, as described in question 5.1 above, must obtain authorisation with the relevant data protection authority. This would include both foreign and local entities and will be determined by who actually determines the purpose and means for processing the personal information.

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.)

At this stage, no formal notification process has been set down.

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

The responsible party is guilty of an offence and liable to a penalty of a fine or imprisonment for a period not exceeding twelve (12) months, or to both a fine and such imprisonment.

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

This is not applicable.

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

A responsible party is required to obtain the prior authorisation only once and not each time that personal information is received or processed, except where the processing departs from that which has been authorised.

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

See question 5.1 above.

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

The Information Regulator is required to inform the responsible party in writing within four (4) weeks of the notification as to whether or not it will conduct a more detailed investigation. In the event that the Information Regulator decides to conduct a more detailed investigation, it must indicate the period within which it plans to conduct this investigation; this period may not exceed thirteen (13) weeks. Upon conclusion of the more detailed investigation, the Information Regulator must issue a statement concerning the lawfulness of the information processing.

6 Appointment of a Data Protection Officer

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

Data Protection Officers do not exist in South Africa. However, the appointment of an Information Officer is mandatory and, in the case of a private body, the Chief Executive Officer ("**CEO**") of a juristic person in South Africa is automatically the Information Officer. The CEO may delegate these powers to a Deputy Information Officer.

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

There is uncertainty in this regard; however, we are hoping that this will be corrected with the issuance of regulations.

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

This is not applicable.

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

This is not applicable.

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

Data Protection Officers do not exist in South Africa; however, an Information Officer's responsibilities includes, *inter alia*:

(a) the encouragement of compliance, by such an entity, with the conditions for the lawful processing of personal information;

(b) dealing with requests made to such an entity pursuant to POPI;

(c) working with the Information Regulator in relation to investigations conducted in relation to such an entity; and

(d) otherwise ensuring compliance by such an entity with the provisions of POPI.

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

Data Protection Officers do not exist in South Africa; however, the appointment of Information Officers must be registered with the Information Regulator prior to the Information Officer taking up their duties.

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.)

POPI provides that the processing of personal information of a data subject for the purpose of direct marketing by means of any form of electronic communication, including automatic calling machines, SMSs or emails, is prohibited, unless the data subject:

(a) has given his consent to the processing; or

(b) is a customer of the responsible party.

The Consumer Protection Act 68 of 2008 ("**Consumer Protection Act**") further specifically provides for the right of every person to privacy, including the right to:

(a) refuse to accept;

(b) require another person to discontinue; or

(c) in the case of an approach other than in person, to pre-emptively block any approach or communication to that person, if the approach or communication is primarily for the purpose of direct marketing.

A person who has been approached for the purpose of direct marketing may demand that the person responsible for initiating the communication desist from initiating any further communication.

A person authorising, directing or conducting any direct marketing must implement appropriate 'opt-out' procedures and must not direct or permit any person associated with that activity to direct or deliver any communication for the purpose of direct marketing to a person who has 'opted-out'. Further, no person may charge a consumer a fee for 'opting-out'.

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

The Information Regulator has not yet been established in South Africa.

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

In terms of the Consumer Protection Act, the Consumer Commission may establish a registry in which any person may register a pre-emptive block, either generally or for specific purposes, against any communication primarily for the purpose of direct marketing. At the time of writing, this registry was not yet established.

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

The penalty for non-compliance with an enforcement notice and infringement notice is liability for an administrative fine of up to ten million rand (R10,000,000) or imprisonment for a period not exceeding ten (10) years, or to both a fine and such imprisonment.

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)?

Any information that would allow for the data subject to be personally identified. In addition, any unsolicited electronic communication must contain an 'opt-out' provision.

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)?

This is not applicable.

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

The Information Regulator has not yet been established in South Africa.

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

See question 7.3 above.

8 Restrictions on International Data Transfers

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

A responsible party in South Africa may not transfer personal information about a data subject to a third party who is in a foreign country, unless:

(a) the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide for a similar level of protection of personal information and restrict the further transfer of the personal information;

(b) the data subject consents to the transfer;

(c) the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request;

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or

(e) the transfer is for the benefit of the data subject, and it is not reasonably practicable to obtain the consent of the data subject to that transfer; and if it were reasonably practicable to obtain such consent, the data subject would be likely to provide it.

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

Companies would conclude a data transfer agreement, which would regulate the foreign transferee's obligations and restrictions in respect of the data.

8.3 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.

See question 5.1 above.

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.)

We do not have corporate whistle-blower hotlines in South Africa as such, but corporate whistle-blowing is governed by the Protected Disclosures Act 26 of 2000 ("**Protected Disclosures Act**"). In terms of the Protected Disclosures Act, employees may make protected disclosures to an employer, legal advisor, member of Cabinet or Executive Council regarding a criminal offence, failure to comply with a legal obligation, miscarriage of justice, endangerment of the health or safety of an individual, damage to the environment, or concealment of any or all of the aforegoing.

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?

By design, protected disclosures under the Protected Disclosures Act are geared at protecting employees from being subjected to an occupational detriment (as defined in the Protected Disclosures Act) as a result of their having made a protected disclosure. There is, however, no strict provision in the Protected Disclosures Act governing anonymity of a person making a protected disclosure.

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.

This is not applicable.

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

This is not applicable as South Africa does not have corporate whistle-blower hotlines.

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

This is not applicable.

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)?

See question 5.1 above.

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

This is not specifically governed by POPI. However, any processing of personal information must comply with the general principles set out in POPI.

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

An employer would need to obtain the consent of an employee in order to process its personal information. This is typically covered in the employee's employment contract.

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

No specific provision of POPI requires a trade union or similar organisation to be consulted or notified. However, the prohibition on processing personal information concerning a data subject's trade union membership does not apply to processing by the trade union to which the data subject belongs or the trade union federation to which that trade union belongs, if such processing is necessary to achieve the aims of the trade union or trade union federation.

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

This is not applicable.

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)?

It is permissible as long as the provisions governing the processing of the personal information as set out in POPI are complied with.

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)?

Where the responsible party uses an operator to process personal information on its behalf, the responsible party must conclude a written contract with the operator in order to ensure that the operator establishes and maintains the security measures as provided for in POPI.

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)?

The utilisation of big data and analytics is permitted only where the data subject has consented to its personal information being processed for this, or where the personal information has been de-identified.

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)?

No specific standards have been set out in POPI.

A general obligation is placed on the responsible party to take reasonable measures to:

(a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

(b) establish and maintain appropriate safeguards against the risks identified;

(c) regularly verify that the safeguards are effectively implemented; and

(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

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.

Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify the Information Regulator as soon as reasonably possible after the discovery of the compromise.

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.

Yes, in addition to the requirements set out in question 13.2 above, the data subject must be notified by the responsible party if a breach in regard to his personal information has occurred.

13.4 What are the maximum penalties for security breaches?

See question 7.4 above.

14 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
The Information Regulator may: (a) summon and enforce the appearance of persons before the Information Regulator and compel them to give oral or written evidence on oath and to produce any records and things that the Information Regulator considers necessary to investigate the complaint, in the same manner and to the same extent as the High Court; (b) administer oaths; (c) receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Information Regulator sees fit, whether or not it is or would be admissible in a court of law; (d) at any reasonable time enter and search any premises occupied by a responsible party; (e) conduct a private interview with any person in any premises entered; and (f) otherwise carry out in those premises any inquiries that the Information Regulator sees fit.	If the responsible party is alleged to have committed an offence in terms of POPI, the Information Regulator may issue an infringement notice, which if the responsible party does not comply with, is liable to an administrative fine not exceeding ten million rand (R10,000,000).	Any person who hinders, obstructs or unlawfully influences the Information Regulator in the performance of his duties is guilty of an offence and is liable to a fine or imprisonment for a period not exceeding ten (10) years, or to both.
The Information Regulator may serve an enforcement notice on the responsible party (after receiving the recommendations of the Enforcement Committee) requiring the responsible party to take the steps specified in the notice within the time period specified.	If the responsible party is alleged to have committed an offence in terms of POPI, the Information Regulator may issue an infringement notice, which if the responsible party does not comply with, is liable to an administrative fine not exceeding ten million rand (R10,000,000).	Failure to comply with an enforcement notice is an offence and is liable to a fine or imprisonment for a period not exceeding ten (10) years, or to both.

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

This is not applicable as the Information Regulator is yet to be established in South Africa.

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?

This is not applicable.

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

This is not applicable.

16 Trends and Developments

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

This is not applicable as POPI is yet to become effective in South Africa (except for certain sections thereof dealing with the establishment of the Information Regulator and Enforcement Committee).

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

This is not applicable as POPI is yet to become effective in South Africa (except for certain sections thereof dealing with the establishment of the Information Regulator and Enforcement Committee).

Tanya Waksman
Eversheds SA
3rd Floor, 54 Melrose Boulevard
Melrose Arch
Melrose North, 2196
Johannesburg
South Africa

Tel: +27 87 358 9857
Email: tanyawaksman@eversheds.co.za
URL: www.eversheds.com

Tanya is a Partner of our firm and practises in our commercial department from our Sandton office. She specialises in commercial and corporate law, banking and finance law, mergers and acquisitions, media, telecommunications and IT law.

Tanya obtained a Bachelor of Social Science degree from the University of Cape Town in 1995. Thereafter, she attended the University of the Witwatersrand where she obtained a Bachelor of Laws degree in 1998.

In 1999, she studied at the University of New South Wales in Sydney, Australia and obtained a Master of Laws degree in Information Technology Law, Media Law and Telecommunications Law.

Tanya advises a number of listed companies and large corporates with all aspects of their business and has extensive experience in advising on corporate restructuring, listings, regulatory compliance and the implementation of mergers and acquisitions both in South Africa and abroad.

EVERSHEDS

Eversheds SA is one of the leading full-service law firms in South Africa. As part of Eversheds International, we can provide clients with the same high standard of legal expertise.

We are a progressive law firm, constantly on the lookout for better ways to provide creative and cost-effective legal and business solutions for our clients. Our approach is personal, combined with the highest professional standards.

We have an extensive blue-chip client base of major domestic and international corporations, banks, financial institutions and state authorities. Our wealth of experience across a wide range of industries enables us to assist with unique challenges of business and other strategic issues that require legal insight and makes us your ideal legal partner in South Africa.

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