International
Comparative
Legal Guides

Digital Business 2020

A practical cross-border insight into digital business law

First Edition

Featuring contributions from:

Anderson Mōri & Tomotsune
Armengaud Guerlain
Bagus Enrico & Partners
BOEHMERT & BOEHMERT
Boga & Associates
Bull & Co
Cliffe Dekker Hofmeyr
Cozen O'Connor P.C.
E & G Economides LLC
Gowling WLG
Greychapel Legal
Hammad & Al-Mehdar Law Firm
Hassan Radhi & Associates
Lewis Silkin
Orchards
Portolano Cavallo
Shin Associates
Sirius Legal
Veirano Advogados
Walder Wyss Ltd

ICLG.com

ISBN 978-1-83918-051-4
ISSN 2732-5237

Published by
global legal group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
info@glgroup.co.uk
www.iclg.com

Group Publisher
Rory Smith

Publisher
James Strode

Senior Editor
Sam Friend

Head of Production
Suzie Levy

Chief Media Officer
Fraser Allan

CEO
Jason Byles

Printed by
Ashford Colour Press Ltd.

Cover image
www.istockphoto.com

Strategic Partners

International Comparative Legal Guides

Digital Business 2020

First Edition

Contributing Editors:
Davey Brennan & Alex Brodie
Gowling WLG

Expert Chapter

Q&A Chapters

From the Publisher

Dear Reader,

Welcome to the first edition of the *ICLG – Digital Business*, published by Global Legal Group.

This publication provides corporate counsel and international practitioners with comprehensive jurisdiction-by-jurisdiction guidance to laws and regulations relating to digital businesses around the world, and is also available at www.iclg.com.

The question and answer chapters, which in this edition cover 21 jurisdictions, provide detailed answers to common questions raised by professionals dealing with digital business laws and regulations.

The publication's opening expert analysis chapter provides further insight into navigating business digitalisation.

As always, this publication has been written by leading lawyers and industry specialists, for whose invaluable contributions the editors and publishers are extremely grateful.

Global Legal Group would also like to extend special thanks to contributing editors Davey Brennan and Alex Brodie of Gowling WLG for their leadership, support and expertise in bringing this project to fruition.

Rory Smith
Group Publisher
Global Legal Group

South Africa


Fatima Ameer-Mia


Christoff Pienaar


Nikita Kekana


Mieke Vlok

Cliffe Dekker Hofmeyr

1 E-Commerce Regulations

1.1 What are the key e-commerce legal requirements that apply to B2B e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2B e-commerce.

The type of e-commerce products and services will determine what licensing and/or authorisation is required and which legislation is relevant.

The Electronic Communications and Transactions Act 25 of 2002 ("**ECTA**") is the primary legislation that regulates electronic communications and electronic transactions in South Africa. ECTA creates recognition for contracts concluded electronically and online and contains a variety of different rules that e-commerce businesses must adhere to. Some of the sections of ECTA apply to B2B e-commerce as well as B2C, and others only apply to B2C e-commerce.

Businesses that provide electronic communications services or electronic communication network services are required to obtain a licence from the Independent Communications of South Africa ("**ICASA**") in terms of the Electronic Communications Act 36 of 2005, unless they are exempted.

Radio frequency licences and type approval of electronic communications equipment and facilities also require ICASA's approval.

1.2 What are the key e-commerce legal requirements that apply to B2C e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2C e-commerce.

In addition to obtaining the licences and approvals mentioned in question 1.1 and needing to comply with ECTA, B2C e-commerce businesses are also required to comply with the Consumer Protection Act 68 of 2008 ("**CPA**").

The CPA applies to transactions taking place within South Africa involving the sale of goods and services to consumers. Consumers include natural and smaller juristic persons whose turnover is less than R2 million per annum. This means that there are instances where the CPA also applies to B2B relationships but for the most part it is confined to B2C relationships.

The CPA heavily regulates transactions between businesses and consumers. For instance, a supplier must not advertise any particular goods or services as being available at a specified price in a manner that may result in consumers being misled or deceived in any respect relating to the actual availability of those goods or services from that supplier, at that advertised price.

Consumers also have the following rights under the CPA:

- the right to opt out of receiving direct marketing communications;
- the right to receive information in plain and understandable language;
- the right to cancel any advance booking, reservation or order for any goods or services to be supplied;
- the right to have any notice drawn to them that:
  - limits the risk or liability of the supplier or any other person;
  - constitutes an assumption of risk or liability by the consumer;
  - imposes an obligation on the consumer to indemnify the supplier or any other person for any cause; or
  - be an acknowledgment of any fact by the consumer.

Under the CPA, a supplier must not offer to supply, or enter into an agreement to supply, any goods or services on terms that are unfair, unreasonable or unjust, or impose any such terms as a condition of entering into a transaction. The CPA also heavily regulates promotional competitions.

Certain provisions in ECTA only apply to B2C e-commerce and specifically deal with consumer protection. These are contained in sections 42-49 of ECTA and consumers may lodge a complaint with the National Consumer Commission against any supplier who fails to comply with these sections. The rights contained in these sections apply to an agreement with a consumer no matter what the governing law of the contract is and cannot be contracted out of.

Section 43 provides a list of information that a supplier must provide to consumers on their website. This includes providing information about security procedures and a privacy policy that deals with payment, payment security and personal information.

Consumers also have the right to cancel any electronic transaction without penalty within seven days after concluding that transaction or after receiving the goods relating to the contract, excluding perishables, accommodation, transport and catering. Consumers can also opt out of receiving unsolicited goods, services and communications.

ECTA further requires a supplier to perform within 30 days unless the parties have agreed to an alternative timeline.

2 Data Protection

2.1 How has the domestic law been developed in your jurisdiction in the last year?

The right to privacy is guaranteed under section 14 of the Constitution of the Republic of South Africa. The Protection of Personal Information Act 4 of 2013 ("**POPIA**") is the legislation that gives effect to this constitutional right.

While some of the provisions of POPIA are in effect, such as the definitions, the appointment the Information Regulator and the procedure for making regulations, the substantive provisions of POPIA are not yet in effect and will only come into effect on a date to be determined by the President. The Information Regulator has been appointed and final regulations have been published. The Information Regulator also requested the President to sign POPIA into law with effect from 1 April 2020, but due to the current COVID-19 pandemic, this has not been a priority. However, the commencement date of POPIA is imminent and is expected to occur in 2020.

Once POPIA comes into full force, responsible parties will be given a one-year grace period (which may be extended) to comply with the obligations and requirements of POPIA without facing penalties for non-compliance.

Despite the substantive provisions of POPIA not being in full force and effect, the Information Regulator issued its first two non-binding directives on processing of personal information on 28 January 2019 and 3 April 2020. The first directive was on the processing of personal information of a voter by a political party and came into effect the year of South Africa's national election.

The Information Regulator's latest directive provides guidance on the processing of personal information in the management and containment of the COVID-19 pandemic. Although not binding, this guidance note provides South Africa with useful insight how to process personal information relating to COVID-19. This is valuable and much needed as government embarks on COVID-19 contact tracing measures and businesses look at processing its employees and contractors' temperatures and other health data relating to their COVID-19 status.

2.2 What privacy challenges are organisations facing when it comes to fintech, AI and digital health?

When it comes to digital health, organisations are typically involved in the processing of information about a person's health life. Under POPIA, this type of information is classified as special personal information and organisations are prohibited from processing this information unless their processing falls into one of the exceptions listed in POPIA. The most relevant of these exceptions is where the persons consent to the processing. Consequently, digital health organisations need to ensure that they have proper measures in place to obtain these persons' (data subjects') consent.

Once POPIA is in full force and effect, organisations within fintech, AI and digital health sectors will also need to ensure that they put measures in place to be able to respond to data subject's requests to obtain, delete and update their personal information and not retain personal information for longer than is necessary. This can sometimes pose a technical challenge to organisations as personal information may be stored in different places within the organisation and data analytics may have been designed so to be dependent on personal information that needs to be destroyed.

2.3 What support are the Government and privacy regulators providing to organisations to facilitate the testing and development of fintech, AI and digital health?

The Intergovernmental Fintech Working Group ("**IFWG**") released its first Fintech Landscaping Report on 22 January 2020 ("**Fintech Report**"). The IFWG includes key governmental bodies within the fintech industry, including the National Treasury and the South African Reserve Bank.

Due to its findings in the Fintech Report, the IFWG has indicated that it intends to introduce a regulatory sandbox. This should enable companies to test their fintech products in a semi-controlled testing environment in collaboration with the relevant regulator while offering temporary relief to these companies from full compliance to fintech regulations.

We are not aware of any similar measures being taken in the digital health or AI sectors at this point in time within South Africa.

3 Cybersecurity Framework

3.1 Please provide details of any cybersecurity frameworks applicable to e-commerce businesses.

South Africa has a hybrid approach to cybersecurity regulation. Cybercrime is regulated through a combination of legislation and the common law. ECTA criminalises cyber-offences such as hacking and phishing and provides for penalties such as fines and imprisonment of up to 12 months.

The Regulation of Interception of Communications and Provision of Communications-related Information Act 70 of 2002 ("**RICA**") regulates and limits the interception and monitoring of direct and indirect communications. This is particularly important for any e-commerce business that hosts their call centres online or records telephone calls or other correspondence.

POPIA also contains provisions regulating the minimum cybersecurity safeguards that need to be in place when processing personal information. Specifically, POPIA requires that entities take 'appropriate, reasonable technical and organisational measures to protect personal information'.

Many crimes that take place online are also crimes under the South African common law such as the crimes of theft, extortion and fraud.

3.2 Please provide details of other cybersecurity legislation in your jurisdiction, and, if there is any, how is that enforced?

Apart from ECTA, POPIA and RICA, Parliament is also in the process of passing a new Cybercrimes Bill [B6 of 2017] ("**Cybercrimes Bill**"), which will introduce new cybercrimes within South Africa and consolidate and codify a number of existing cybercrimes, as well as regulate the investigation and prosecution of such offences.

The Cybercrimes Bill was passed by the first parliamentary body, the National Assembly on November 2018. It is currently undergoing the public participation process within the second parliamentary body, the National Council of Provinces ("**NCOP**"). After the public participation process, the NCOP will vote on whether or not to pass the Cybercrimes Bill.

4 Cultural Norms

4.1 What are consumers' attitudes towards e-commerce in your jurisdiction? Do consumers embrace e-commerce and new technologies or does a more cash-friendly consumer attitude still prevail?

Currently the contribution from e-commerce sales to overall retail sales is still relatively low and is estimated to be below 2% of the total annual sales.

However, e-commerce is steadily growing and the current COVID-19 pandemic is also likely to make more consumers reliant on e-commerce. There are however certain industries and sub-industries that already show high consumer affinity towards e-commerce including the digital health sector and the e-taxi industry.

4.2 Do any particular payment methods offer any cultural challenges within your jurisdiction? For example, is there a debit card culture, a direct debit culture, a cash on delivery type culture?

Originally e-commerce businesses introduced a credit card culture for the payment of goods and services. However, the industry rapidly introduced a variety of different payment methods including mobile payments such as Snapscan and cash on delivery. These additional methods were introduced as a vast number of South Africans do not have credit cards and even traditional banking facilities so a credit card culture would greatly hinder digital businesses' ability to grow.

4.3 Do home state retailer websites/e-commerce platforms perform better in other jurisdictions? If so, why?

The vast majority of e-commerce platforms in South Africa are home state retailers rather than international platforms. A few reasons for this is because international platforms tend to have high delivery/shipping costs, need to go through customs control (and customs duty payable on such imported goods are typically quite high) and their offerings are typically quoted in a currency such as United States Dollars or Euros, of which the exchange rate fluctuations tend to be volatile against the South African currency.

4.4 Do e-commerce firms in your jurisdiction overcome language barriers to successfully sell products/services in other jurisdictions? If so, how and which markets do they typically target and what languages do e-commerce platforms support?

Currently cross-border e-commerce transactions from South Africa are rare as South African e-commerce businesses tend to focus exclusively on the South African market. One of the reasons for this are the strict customs and exchange controls regulations.

South African e-commerce businesses typically only publish their website content in English and communicate in English. Thus, these firms are not overcoming any language barriers that may exist with offering services to non-English speaking customers.

4.5 Are there any particular web-interface design concepts that impact on consumers' interactivity? For example, presentation style, imagery, logos, currencies supported, icons, graphical components, colours, language, flags, sounds, metaphors, etc.

As many South Africans access websites on their mobile phones, it is critical that websites interfaces are mobile friendly. Successful digital businesses also tend to have a simple and easy to navigate website. Many consumers want websites to have responsive onsite search functionality.

5 Brand Enforcement Online

5.1 What is the process for online brand enforcement in your jurisdiction?

Online brand enforcement can be divided into a business' brand protection due to its rights at law and brand protection through contract enforcement.

At law, a business has a number of options to protect its brand. For instance, South African copyright law protects a closed list of works, including computer programs, (software) from copyright infringement and affords owners of these works certain exclusive rights. These rights include the right to make an adaption and license the work. Trademarks, particularly registered trademarks, also enable businesses to protect its brand through prohibiting others from copying its slogans, logos, business name and products. Digital businesses also ensure that their online brand is protected by registering domain names (url) for their websites. In South Africa, domain names end with co.za.

Digital businesses typically also include additional restrictions in their terms and conditions that protect their brand and products. For instance, a business may restrict a client to only use the licensed software for private and non-commercial use.

Digital businesses will typically enforce their brand protection by sending a letter of demand to parties that are infringing upon their intellectual property rights and/or violating their terms and conditions. If an infringing party does not agree to stop their infringing behaviour then that digital business may institute court proceedings against the infringing party. Typical remedies for brand infringement include interdicting (injuncting) the infringer from committing the infringing act and awarding damages in favour of a digital business for any losses and harm suffered.

5.2 Are there any restrictions that have an impact on online brand enforcement in your jurisdiction?

A big restriction on online brand enforcement is territorial restrictions. Digital businesses typically operate through a website which is accessible anywhere in the world. Thus, it is possible that a party within a different country may copy that business' software or otherwise harm a business' brand from abroad.

The South African business may struggle to enforce their brand and intellectual property rights outside of South Africa for a number of reasons. One of which may be that the jurisdiction where the infringer is domiciled does not have equivalent intellectual property rights as those contained within South Africa. Another is that the relevant country may be unwilling to recognise and enforce a foreign judgment.

Another common reason is even if a jurisdiction has similar copyright laws to those afforded under South African law, and/or would recognise and enforce a South African judgment against an infringer, it may be too expensive and impractical for a business to enforce its brand abroad.

6 Data Centres and Cloud Location

6.1 What are the legal considerations and risks in your jurisdiction when contracting with third party-owned data centres or cloud providers?

The key legal considerations to be aware of when contracting with third-party data centres or cloud providers are ensuring that:

- they adhere to the data protection requirements set out in POPIA;
- they have appropriate data security including encryption and data recovery mechanisms in place; and
- the ownership of the data and any data analytics produced from the business' data using the cloud services is definitively determined.

6.2 Are there any requirements in your jurisdiction for servers/data centres to be located in that jurisdiction?

Data centres and servers do not need to be located within South Africa, but where the data stored on the cloud contains personal information, this needs to adhere to POPIA.

Section 72 of POPIA limits the instances when a responsible party, i.e. a business, can transfer personal information to a third party, e.g. cloud provider, outside of South Africa. This is limited to when:

- the third party who is the recipient of the information is subject to a law, binding corporate rules or a binding agreement that provide an adequate level of protection that:
  - effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject; and
  - include provisions that are substantially similar to clause 72;
- the data subject consents to the transfer;
- the transfer is necessary for the performance of a contract between the data subject and responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request;
- the transfer is necessary for the performance or conclusion of a contract concluded in the interest of the data subject between a third party and the responsible party; or
- 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 consent.

7 Trade and Customs

7.1 What, if any, are the technologies being adopted by private enterprises and government border agencies to digitalise international (cross-border) trade in your territory?

Private entities are increasingly using technology to overcome the challenges consumers may face when engaging in cross-border transactions, particularly challenges related to cross-border payments and cross-border logistics.

To this end there is an increase in payment technology innovations, such as companies offering contactless, instant cross-border payments at fixed, transparent tariffs by utilising a blockchain network. This serves as an alternative to the traditional manual and costly cross-border payment.

There has also been innovation in the delivery and logistics landscape, with one local player offering same-day delivery of groceries purchased in South Africa to customers in Zimbabwe. Another local logistics company has piloted last-mile delivery of goods purchased in South Africa to neighbouring countries such as Namibia, Botswana, Lesotho and Swaziland. The customer pre-selects a drop-off point for the delivery, such as a retailer in a public shopping mall, and the courier delivers the parcel to this drop-off point whereafter the customer can collect their parcel on their own time by presenting a unique code.

Early in 2020 the commissioner of South Africa's tax authority, the South African Revenue Service, affirmed the authority's commitment to "in customs in particular work with other governments to implement existing memorandums of understanding that allow for exchange of trade information to help reconcile their export data with our import data and address data asymmetries".

It added that it aims to "deploy artificial intelligence to derive better insights, highlight relevant risks, ensure more intelligent responses, and improved outcomes" and that to this end it is recruiting a chief data scientist and chief technology innovation officer.

Government agencies such as the tax authority have thus proclaimed their intention to prioritise technology to facilitate cross-border transactions; however, no specific technology has been deployed yet.

7.2 What do you consider are the significant barriers to successful adoption of digital technologies for trade facilitation and how might these be addressed going forwards?

The adoption of digital technology in cross-border trade is mainly hampered by bureaucracy and legislation which predates the rise of cross-border e-commerce.

The restrictions imposed by the authorities often make it difficult and costly for consumers and private entities to engage in international transactions. South Africa's Customs and Excise Act was first promulgated in 1964 and, though various amendments have been made since, it is not well aligned to the current e-commerce age. The Act places restrictions on the number of international purchases a South African consumer may engage in for personal use during one calendar year, as well as the value of these transactions, and obliges ordinary consumers to register as importers once they exceed these generally low thresholds.

This discourages consumers from engaging in international transactions, and in turn limits the growth of private companies in this sector. Legislative reform is therefore a key step to improving the use of digital technology in cross-border trade. The sooner it becomes easier for ordinary consumers to transact abroad, the sooner private companies can cater to this demand and innovate to create new technologies for this market.

8 Tax Treatment for Digital Businesses

8.1 Can you give a brief description of any tax incentives of particular relevance to digital businesses in your jurisdiction? These could include investment reliefs, research and development credits and/or beneficial tax rules relating to intellectual property.

A research and development ("**R&D**") tax incentive is provided for in terms of South Africa's Income Tax Act. The incentive's aim is to encourage investment into and the growth of the scientific and technological R&D sector in South Africa. Eligible companies can claim a 150% deduction in respect of all qualifying R&D expenditure once approval for the specific R&D project has been obtained from the Department of Science and Technology. The initiative is, however, set to end in October 2022 and is therefore only applicable in respect of R&D expenditure incurred before 1 October 2022.

Companies can also take advantage of the tax authority's employment tax incentive, which provides tax benefits for companies employing young and less experienced workers, as well as the tax benefits related to having their company classified as a Small Business Corporation.

With regard to South Africa's value-added tax ("**VAT**"), i.e. a goods and service tax, a taxable supply of services relating to intellectual property rights is zero-rated (i.e. subject to VAT at the rate of 0%) if, and to the extent that, the rights are for use outside the Republic.

8.2 What areas or points of tax law do you think are most likely to lead to disputes between digital businesses and the tax authorities, either domestically or cross-border?

One of the most contentious points between digital business and the local tax authorities is the leveraging of VAT. The current VAT rate is 15%.

In 2014, the South Africa tax authorities published regulations pursuant to the Value Added Tax Act of 1991, requiring foreign suppliers of electronic services (e-services) to South African recipients to register as VAT vendors in South Africa if they meet certain revenue and other requirements.

With effect from 1 April 2019, revised regulations were published to prescribe and clarify the e-services supplied by foreign suppliers to South African consumers which are subject to VAT. The revised regulations significantly broadened the scope of what constitutes e-services and the regulations now to apply to *any services supplied by means of an 'electronic agent', 'electronic communication' or the 'internet' for any consideration*. Subject to certain specific exclusions, the effect of the revised regulations is that virtually all services that are supplied by way of electronic means, such as, for example, cloud computing, computer software and any online services, are now included as 'e-services'. Furthermore, intermediaries who facilitate the supply of e-services or who provide their platforms to foreign suppliers for rendering the e-services to South African customers, and who are responsible for invoicing and collecting payment for the e-services, are also required the register for VAT in South Africa. A simplified VAT registration process has been introduced for foreign e-services suppliers.

9 Employment Law Implications for an Agile Workforce

9.1 What legal and practical considerations should businesses take into account when deciding on the best way of resourcing work in your jurisdiction? In particular, please comment on the advantages and disadvantages of the available employment status models.

Businesses should take note that South African employment contracts are largely regulated by the Basic Conditions of Employment Act of 1997 and ancillary legislation such as the Labour Relations Act of 1995 and the Employment Equity Act of 1998 grant employees additional rights in certain instances. South Africa has a designated labour court as well as a commission providing for the conciliation, mediation and arbitration of labour disputes, free of charge. South African legislation makes provision for a minimum wage.

Various employment models are utilised, ranging from permanent, fixed term or part-time employees to independent contractors. Full-time employees are advantageous in the sense that they are a dedicated resource; however, full-time employees can be costly from an on-boarding, recruitment and benefits provision perspective. Part-time or contract workers may be more cost-effective; however, an over-reliance on these workers can be disruptive to business continuity if these workers are constantly changing. Businesses should note that the Labour Relations Act of 1995 contains specific provisions on what constitutes an employee and that the courts have taken action against employers who treat workers as "*independent contractors*" instead of employees in an effort to avoid certain obligations the employer has towards an employee.

A popular strategy for businesses is to employ full-time personnel for core, ongoing duties and utilise part-time or contract workers as and when needed for specific tasks. Many companies are also outsourcing functionalities such as accounting, human resources, information systems and advisory services in an effort to cut costs.

9.2 Are there any specific regulations in place in your jurisdiction relating to carrying out work away from an organisation's physical premises?

There are no specific regulations relating to the place of work generally. Most employers include a standard term in their contracts of employment that employees agree to work at a specific premises or such other location as may be designated by the employer from time to time.

10 Top 'Flags' for Doing Business as a Digital Business in Different Jurisdictions

10.1 What are the key legal barriers faced by a digital business operating in your jurisdiction?

One of the biggest legal barriers to digital business within South Africa is ensuring that digital businesses are appropriately licensed for the goods and services that they are offering.

ECTA governs most aspects of online business so it is critical for digital businesses to ensure that they comply with ECTA. For instance, section 43(1) of ECTA requires a supplier of goods

or services by way of an electronic transactions to provide its consumers with a wide range of information about its business and offerings on its website including:

- the business' details such as its full name, legal status, physical address, email address and telephone number;
- description of the goods and services offered; and
- the business' return, exchange and refund policy.

A digital business must also be aware of any industry-specific rules and regulations that apply to it. For instance, a business offering digital health must ensure that it has considered and complies with the National Health Act 61 of 2003, the Medicines and Related Substances Act 101 of 1965, the Medicines and Related Substances Amendment Act, 14 of 2015 and the Health Professions Act No. 56 of 1974.

10.2 Are there any notable advantages for a digital business operating in your jurisdiction?

A notable advantage to digital business operations is a lower maintenance cost as typically digital businesses need to spend less on premises because fewer client interactions take place onsite and data is typically stored on the cloud or on servers rather than physically.

The COVID-19 pandemic has also demonstrated that digital businesses are proving to be more adaptable and resilient to unexpected and rapid changes. For instance, many digital businesses already had infrastructure in place to allow their staff to work remotely and continue with their operations almost completely online or telephonically, subject to any governmental restrictions.

11 Online Payments

11.1 What regulations, if any, apply to the online payment sector in your jurisdiction?

The South African Reserve Bank ("**SARB**") is mandated in terms of the South African Reserve Bank Act, 90 of 1989 ("**SARB Act**") to oversee the regulation of the national payment systems of South Africa ("**NPS**"). This includes the regulation and supervision of payment, clearing and settlement systems, and to ensure the safety and efficiency of the NPS. The National Payment System Act, 78 of 1998 ("**NPS Act**") mandates the SARB to recognise a payment system management body to organise, manage and regulate participants in the NPS. Currently, the Payments Association of South Africa ("**PASA**") is recognised as the payment system management body by the SARB.

Banks can process online payments in terms of their banking licence. Non-banks that are beneficiary service providers or payment service providers need to obtain a third-party payment provider ("**TPPP**") licence. In order to get a TPPP licence, they need to enter into a sponsoring arrangement with a registered South African bank.

Entities that operate as technical service providers ("**TSP**") and process money using electronic means to two or more persons to allow such persons to make payments and/or receive payment from one account to another but do not hold the funds themselves need to obtain a system operator licence from PASA.

11.2 What are the key legal issues for online payment providers in your jurisdiction to consider?

A key legal issue is ensuring that the payment provider is appropriately licensed for the type of payment processing that it offers, and it remains appropriately licensed. Each year the payment provider is required to pay a renewal fee and ensure that any conditions accompanying their licence are maintained, e.g. having a proper disaster recovery plan.

Further as many online payment providers process card payments of either MasterCard or Visa card, it is critical for these providers to ensure that they comply with the stringent card scheme rules and make sure that they are Payment Card Industry Data System Security ("**PCI DSS**") certified.

Fatima Ameer-Mia is a Director in the Technology, Media & Telecommunications practice in Johannesburg. She specialises in commercial matters and transactions with a technology or intellectual property related focus – such as software development, licensing, outsourcing, the commercialisation of intellectual property and a wide range of managed services. Her expertise extends to fintech, health-tech, insure-tech and data protection across a diverse range of industry sectors, especially financial services, retail and healthcare. She also has a special interest in the fields of cybercrime, information security and artificial intelligence.

Cliffe Dekker Hofmeyr
1 Protea Place, Sandton
Johannesburg, 2196
South Africa

Tel: +27 11 562 1898
Email: fatima.ameermia@cdhlegal.com
URL: www.cliffedekkerhofmeyr.com

Christoff Pienaar is a Director and the National Head of Technology, Media & Telecommunications at Cliffe Dekker Hofmeyr. He advises on commercial, information technology and intellectual property law. He specialises in information technology and commercial matters and has particular expertise in payment systems, technology outsourcing, business process outsourcing, systems integration, hardware acquisitions and maintenance, IT consultancy services, managed services, disaster recovery services, software development and software licensing and support transactions. Christoff also advises on general commercial and intellectual property issues across a diverse range of industry sectors, especially financial services.

Cliffe Dekker Hofmeyr
11 Buitengracht Street
Cape Town
South Africa

Tel: +27 21 481 6300
Email: christoff.pienaar@cdhlegal.com
URL: www.cliffedekkerhofmeyr.com

Nikita Kekana is an Associate in Cliffe Dekker Hofmeyr's Technology, Media & Telecommunications practice. Nikita specialises in data protection law, information technology, intellectual property and commercial law. Nikita regularly advices clients within the digital health, film, IT and fintech industries. Nikita also has a keen focus on advising clients on their online business operations and on cross-border data transfers.

Cliffe Dekker Hofmeyr
11 Buitengracht Street
Cape Town
South Africa

Tel: +27 21 481 6300
Email: nikita.kekana@cdhlegal.com
URL: www.cliffedekkerhofmeyr.com

Mieke Vlok is a candidate attorney in Cliffe Dekker Hofmeyr. Mieke has experience in commercial transactions and advising clients on information technology contracts across a variety of industries.

Cliffe Dekker Hofmeyr
11 Buitengracht Street
Cape Town
South Africa

Tel: +27 21 481 6300
Email: mieke.vlok@cdhlegal.com
URL: www.cliffedekkerhofmeyr.com

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Family Law
Financial Services Disputes
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State 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 Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms
Workplace Pensions

@ICLG_GLG

The International Comparative Legal Guides are published by:

global legal group