ICLG

The International Comparative Legal Guide to:

Cybersecurity 2018

1st Edition

A practical cross-border insight into cybersecurity work

Published by Global Legal Group, with contributions from:

Allen & Overy
Angara Abello Concepcion Regala & Cruz Law Offices
Baker McKenzie
Boga & Associates
BTG Legal
Christopher & Lee Ong
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
ENSafrica
Erkelens Law
Eversheds Sutherland
Holland & Hart LLP
JIPYONG
Josh and Mak International
King & Wood Mallesons
Lee, Tsai & Partners Attorneys-at-Law
Maples and Calder
MinterEllison
Mori Hamada & Matsumoto
Niederer Kraft & Frey Ltd.
R&T Asia (Thailand) Limited
Rajah & Tann Singapore LLP
Shibolet & Co.
Simmons & Simmons LLP
Udo Udoma & Belo-Osagie

glg
global legal group

global legal group

Contributing Editors
Nigel Parker & Alex Shandro, Allen & Overy LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Sub Editor
Oliver Chang

Senior Editors
Suzie Levy, Rachel Williams

Chief Operating Officer
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

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.
October 2017

ISBN 978-1-911367-77-2
ISSN 2515-4206

Strategic Partners

General Chapters:

Country Question and Answer Chapters:

Kosovo

Sokol Elmazaj

Delvina Nallbani

Boga & Associates

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Law No. 03/L –166 "On prevention and fight of the cyber crime" ("Cyber Crime Law") provides for criminal offences related to the misuse of computer systems and computer data, although it does not provide a literal denomination of the criminal offences listed below.

Hacking (i.e. unauthorised access)

Subject to the Cyber Crime Law, unauthorised access to computer systems constitutes a criminal offence punishable by imprisonment for up to three years. Unauthorised actions are classified actions performed by a person: (i) who is not authorised by law or contract; (ii) who exceeds the limits of his/her authorisation; and/or (iii) has no permit and is not competent and qualified to use, administer or control a computer system or conduct scientific research on a computer system.

If such an offence is committed for the purpose of obtaining computer data or violates computer security measures, penalties provided by law are higher and such offences are punishable by imprisonment for up to four years and five years, respectively.

In addition, the Criminal Code (Law No. 04/L-082) provides for the criminal offence of unauthorised access into computer systems. In this regard, whoever, without authorisation and in order to gain unlawful material benefit for himself or another person or to cause damage to another person, alters, publishes, suppresses or destroys computer data or programs, or in any other way enters another's computer system, is punished by a fine and up to three years of imprisonment. If the offence results in material gain exceeding the amount of 10,000 Euros or material damage exceeding the amount of 10,000 Euros, the perpetrator shall be punished by a fine and by imprisonment of up to five years.

Denial-of-service attacks

The serious hindrance of the functioning of computer systems, performed by entering information, transferring, changing, removing or destroying computer data or limiting unauthorised limit to access to such data, is stipulated as a criminal offence pursuant to the Cyber Crime Law, and the perpetrator is liable to imprisonment for up to three years. Such offence shall be punished by imprisonment for up to five years if committed by a member of a criminal organisation.

Phishing

We have not identified a criminal offence provided by the Cyber Crime Law or other applicable laws that would represent phishing. However, each criminal activity that aims to misuse computer systems or computer data should be considered individually to establish whether it constitutes a criminal offence provided for by the Cyber Crime Law or any other applicable law.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

We have not identified a criminal offence provided by the Cyber Crime Law or other applicable laws that would constitute infection of IT systems with malware. However, each criminal activity that aims to misuse computer systems or computer data should be considered individually to establish whether it constitutes some other criminal offence provided for by the Cyber Crime Law or any other applicable law.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

Pursuant to the Cyber Crime Law, the illegal production, sale, import, distribution or making available, in any form, of any equipment or computer program designed and adapted for the purpose of committing any criminal offence is punishable by imprisonment from one to four years.

Further, the illegal production, sale, import, distribution or making available, in any form, of passwords, access codes or other computer information that would allow full or partial access to a computer system for the purpose of committing any criminal offence shall be punishable by imprisonment from one to five years.

In addition, the illegal possession of equipment, computer programs, passwords, access codes or computer information for the purpose of committing any criminal offence is punishable by imprisonment from one to six years.

An attempt to commit this criminal offence is also punishable by imprisonment, ranging from three months to one year.

Identity theft or identity fraud (e.g. in connection with access devices)

We have not identified any criminal offence provided for by the Cyber Crime Law or other applicable laws that would constitute identity theft or identity fraud. However, as mentioned above, such criminal activities should be assessed individually.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Pursuant to the Criminal Code (Law No. 04/L-082), an act of avoiding any of the effective technological measures to safeguard technology or the removal or alteration of electronic rights for data management, as provided for by the Law "On copyright and related rights", shall be punishable by imprisonment for up to three years.

Subject to the Law "On copyright and related rights" (Law No. 04/L-065), violation of the rights protected by this law would be considered if a person processes, imports for distribution, sells, lends, advertises for sale or lease or keeps for commercial technological purposes a computer program, or carries out services without authorisation, and if such actions: (i) are advertised or traded especially for the purpose of avoiding effective technological measures; (ii) have evident commercial purpose or have been used solely for avoiding effective technological measures; and (iii) are designed, produced, adapted or processed primarily with the purpose of avoiding effective technological measures. An effective technological measure is considered as any technology, computer program or other means intended to prevent or remove a violation of a protected right. Pursuant to the Criminal Code (Law No. 04/L-082), an act of avoiding any of the effective technological measures to safeguard technology or the removal or alteration of electronic rights for data management shall be punishable by imprisonment for up to three years.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

In addition to the criminal offences listed above, the Cyber Crime Law also provides for the following criminal offences related to computer systems and computer data: the unauthorised entry of data; change or deletion of computer data; and the unauthorised limitation of access to such a data resulting in inauthentic data.

Also, causing a loss in assets to another person by entering information, changing or deleting computer data by means of access limitation to such a data, or any other interference into the functioning of a computer system with the purpose of ensuring economic benefits for himself or for someone else, shall be punishable with up to 10 years of imprisonment.

Failure by an organisation to implement cybersecurity measures

We have not identified such a criminal offence provided for by the applicable legislation.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The abovementioned laws that stipulate criminal offences apply to the Kosovo territory. In addition, subject to article 115 of the Criminal Code (Law No. 04/L-082), the criminal legislation of the Republic of Kosovo will also apply to persons who have committed such criminal offences outside the territory of Kosovo, if, according to an international agreement by which Kosovo is bound, such criminal offences should be prosecuted even though committed abroad.

Criminal legislation of the Republic of Kosovo shall also apply to any Kosovo citizen or a foreigner who commits a criminal offence outside the territory of the Republic of Kosovo if the criminal offence is also punishable in the country where the offence was committed. In case of foreigners, these provisions shall apply if the foreigner is found in the territory of Kosovo or has been transferred to Kosovo.

However, the criminal proceedings against a Kosovo citizen or a foreigner for criminal offences committed outside Kosovo territory will not be undertaken if the perpetrator has fully served the punishment imposed in another jurisdiction, has been acquitted by a final judgment and/or released from punishment or punishment has become statute-barred and in cases where criminal proceedings may only be initiated upon the request of the injured party and such a request has not been filed.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

Subject to article 8 of the Cyber Crime Law, for a category of computer systems to which access is restricted or completely forbidden, the owners and administrators of such a computer system are obliged to clearly and automatically warn the user of this computer system, and to provide him/her with information, as well as conditions of use, or forbiddance to use this computer system and legal consequences for unauthorised access to this computer system. Failure to comply with such an obligation is considered a misdemeanour and the perpetrator is punished with a fine ranging from 500 to 5,000 Euros.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

The Criminal Code provides that issuing blank or false cheques and the misuse of bank or credit cards constitutes a criminal offence. Such an offence is defined as an act committed for the purpose of gaining unlawful material benefit for the perpetrator or for another person, by issuing or placing into circulation cheques for which the perpetrator knows are not covered by material means. The placing of false cheques or counterfeit credit cards is punished by a fine and imprisonment for up to three years. In relation to prosecution of this criminal offence in a cybersecurity context, there is a case pending before Kosovo courts where the defendant has been prosecuted for violation of the Cyber Crime Law, specifically for the possession or use of passwords, hardware, software or other tools to commit cybercrime.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import / export controls, among others.

The Applicable Laws relevant to cybercrime are listed below:

Law No. 03/L –166 "On prevention and fight of the cyber crime"; Law No. 04/L-082 "Criminal Code of The Republic Of Kosovo", as amended by Law No. 04/L-129 and Law No. 04/L-273; Law No. 03/L-050 "On the establishment of the Kosovo security council"; Law No. 04/L-145 "On information society government bodies"; Law No. 04/L-094 "On the information society services"; Law No. 04/L-109 "On electronic communications"; Law No. 05/L-030 "On interception of electronic communication"; Law No. 03/L –172 "On the protection of personal data"; Law No. 04/L-076 "On police"; Law No. 03/L-142 "On public peace and order"; Law No. 03/L063 "On Kosovo intelligence agency"; Law No. 04/L-149 "On the execution of penal sanctions", as amended by Law No. 05/L-129; Law No. 04/L-065 "On copyright and related rights"; Law No. 03/L-183 "On the implementation of international sanctions"; Law No. 04/L-213 "On international legal cooperation in criminal matters"; Law No. 04/L-052 "On international agreements"; Law No. 04/L-072 "On controlling and supervising state borders", as amended by Law No. 04/L-214; Law No. 04/L-093 "On banks, microfinance institutions and non bank financial institutions"; Law No. 04/L-064 "On Kosovo agency on forensic"; Law No. 04/L-198 "On the trade of strategic goods"; Law No. 04/L –004 "On private security services"; Law No. 03/L-046 "On the Kosovo security force";

Code No. 03/L-109 "Customs and excise code of Kosovo"; Law No. 04/L-099 "On amending and supplementing the customs and excise code in Kosovo"; and Law No. 03/L –178 "On classification of information and security clearances".

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, how (and according to what timetable) is your jurisdiction expected to implement the Network and Information Systems Directive? Please include details of any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

Kosovo is not an EU member; however, the Ministry of Internal Affairs has adopted the State Strategy for Cyber Security and the Action Plan for 2016 to 2019, drafted based on European Union practices and policies, in addition to the assessments of law enforcement agencies and governmental institutions.

The Kosovo Government has also made the Kosovo Police available as a permanent contact point for international cooperation in the field of cybercrime. In this regard, the Kosovo Police should ensure ongoing international cooperation and assistance in the field of cybercrime, order data retention and confiscation of equipment containing data, as well cooperate with all competent Kosovo authorities while undertaking execution actions.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

The Cyber Crime Law provides that authorities and public institutions with competence in this area, service providers, non-governmental organisations and civil society representatives should carry out activities and programmes for the prevention of cybercrime and develop policies, practices, measures, procedures and minimum standards for the security of computer systems and should also organise information campaigns on cybercrime and risks for computer system users.

The Ministry of Justice, the Ministry of Internal Affairs, the Ministry of Transport and Communications, the Ministry of Public Services, and the Kosovo Intelligence Services shall develop special training programmes for personnel for the purpose of preventing and fighting cybercrime in accordance with specific competencies.

It is to be noted that the Government of Kosovo has presented a draft Law on Cyber Security which should be enacted within 2018. This law should specify the obligations and safety measures to be taken by the responsible natural or legal persons in the field of cybersecurity.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import / export controls of encryption software and hardware.

We have not identified any provisions that could lead to conflicts of laws issues. However, in certain cases, the provisions of Law No. 05/L -030 "On interception of electronic communications", which govern the procedures and conditions for authorised interception of electronic communications, may come into conflict with the measures for surveillance, detection, prevention or mitigation of an Incident by authorised authorities in the cybercrime area.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

There is no obligation to report information related to Incidents to a special authority in Kosovo. However, the Cyber Crime Law provides that the Ministry of Justice in cooperation with the Ministry of Internal Affairs shall continuously maintain and supplement the database on cybercrime.

In principle, in order to report any criminal offence, a criminal complaint may be filed by any person to the police station in the area where the crime was committed or to the competent state prosecutor in writing, by technical means of communication or orally. For practical reasons, criminal offences are typically reported to the police station.

After receiving information of a suspected criminal offence, the police shall investigate whether there is reasonable suspicion that a criminal offence prosecuted *ex officio* has been committed. The police shall investigate a criminal complaint and shall take all the necessary steps (i.e. to locate the perpetrator, to prevent, detect and preserve traces and other evidence, to collect all the information that may be of use in criminal proceedings, etc.). In order to perform these tasks, the police are authorised, under the provisions of the Criminal Procedure Code (Law No. 04/L-123), to gather information from individuals, to take all the necessary steps to establish the identity of the persons, and to interview witnesses or possible suspects, etc.

Based on such collected information, the police drafts the criminal complaint and submits it to the competent state prosecutor. The public prosecutor is obliged to act according to the criminal complaint, i.e. to initiate proceedings (file an indictment) or to dismiss the criminal complaint.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

The applicable legislation is silent in this regard.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Subject to the Cyber Crime Law, the prosecutor is obliged to notify

in writing, by the end of the investigations, the persons who are under investigation.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

The applicable legislation does not address this issue.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The State Prosecutor and the Courts are the institutions responsible for the prosecution and punishment of perpetrators of criminal offences and for the confiscation of property acquired through criminal offences.

Also, listed below are institutions relevant to the cybercrime area:

- The Ministry of Internal Affairs is responsible for the drafting and monitoring of policies and legislation in the field of overall security and cybersecurity.
- The Kosovo Police, as a law enforcement agency, has the primary responsibility in combating all forms of cybercrime within the Cybercrime Sector and for implementing specific supporting structures. The Kosovo Police also serves as a contact point for international cooperation in the field of cybercrime.
- The Kosovo Security Council Secretariat, as an integral part of the Kosovo Security Council, prepares periodic reports for the Government of the Republic of Kosovo and the Kosovo Security Council dealing with security policy issues.
- The Kosovo Intelligence Agency identifies threats that endanger Kosovo's security, such as the threat to territorial integrity, institutional integrity, constitutional order, stability and economic development, as well as threats to global security to the detriment of Kosovo.
- The National Agency for the Protection of Personal Data ensures that controllers respect their obligations regarding the protection of personal data and that data subjects are informed about their rights and obligations in accordance with the Law "On protection of personal data". The Ministry of Justice, the Ministry for the Kosovo Security Force, the Ministry of Economic Development, the Ministry of Foreign Affairs, the Ministry of Finance, as well as the Regulatory Authority of Electronic Data and Postal Communications and the Information Society Agency contribute to cybersecurity in their relevant fields.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

There are no penalties provided for by the applicable legislation.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

We are not aware of any enforcement actions taken in this area.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

There is no consolidated practice in the area of cybercrime to make this assessment.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

There are no specific requirements as regards to cybersecurity in different organisations. However, as regards to the telecommunication sector, there are specific obligations for the purpose of criminal proceedings for entrepreneurs of public electronic communications services and networks based on the Law "On electronic communications" (Law No. 04/L-109). As regards to the financial sector, financial institutions in Kosovo are bound by the provisions of the Law "On the prevention of money laundering and combating financing of terrorism" (Law No. 05/L-096), which provides measures and procedures for detecting and preventing criminal offences of money laundering and combating terrorist financing.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

We have not identified such circumstances based on the applicable legislation.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

There is no such responsibility provided under the Applicable Laws for companies.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

No, they are not.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

No, they are not.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

Civil actions that may be brought would be those of claiming compensation of damages in virtue of the Law "On obligations relationship" (Law No. 04/L-077). In that case, the culpability of a person that has caused damages in relation to any Incident should be proven.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

From the review of some of the published decisions of the Basic Courts and the Supreme Court adopted during 2016 and 2017, we have not identified any decision adopted in this respect. Based on media reports, there have been several cases of prosecution for possession or use of passwords, software or other tools to commit cybercrime, prosecuted in connection with the criminal offence of abuse of banks and credit cards.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

There are no such liabilities provided under Kosovo law.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Such a type of insurance does not exist in practice.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no such regulatory limitations provided by the Applicable Laws.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

There are no such requirements provided by the applicable legislation.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

The Law "On witness protection" (Law No. 04/L-015) may limit the reporting of Incidents. Such a law provides for special and urgent measures and procedures for witness protection if there is a serious threat to a person and the person's close relatives and if that person accepts to cooperate closely with the Courts or investigatory authorities.

Defence measures may be applied before, during and after criminal proceedings for the person considered to be endangered, with regard to the investigation of the following criminal offences:

i. A criminal offence against Kosovo, its citizens and its inhabitants.
ii. A criminal offence against international law.
iii. A criminal offence against the economy.
iv. A criminal offence against official duty.
v. A criminal offence for which a punishment of five or more years of imprisonment is prescribed by law.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

Pursuant to the Criminal Procedure Code (Law No. 04/L-123), the state prosecutor may undertake investigative actions or authorise the police to undertake investigative actions regarding the collection of evidence. In the latter case, the police shall investigate criminal offences and shall take all the steps necessary to locate the perpetrator, to prevent the perpetrator or his/her accomplice from hiding or fleeing, to detect and preserve traces and other evidence of the criminal offence and objects which might serve as evidence, and to collect all the information that may be of use in the criminal proceedings.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are no such requirements.

Sokol Elmazaj
Boga & Associates
Nene Tereza Str. Entry 30
No. 5 Pristina
Kosovo

Tel: +381 38 223 152
Email: selmazi@bogalaw.com
URL: www.bogalaw.com

Sokol joined Boga and Associates in 1996.

He is a Partner of the firm and Country Manager for Kosovo.

He has extensive expertise in corporate, mergers and acquisitions, project financing, privatisation, real estate projects, energy, telecommunication, and dispute resolution. He is continuously involved in providing legal advice to numerous project-financing transactions, mainly on concessions and privatisations, with a focus on energy and infrastructure, both in Albania and Kosovo.

Sokol also conducted a broad range of legal due diligences for international clients considering to invest in Albania or Kosovo in the fields of industry, telecommunications, banking, real estate, etc.

He is an authorised trademark attorney and has an expertise in trademark filing strategy and trademark prosecution, including IP and litigation issues.

Sokol is continuously ranked as a Leading Lawyer in the well-known guides *Chambers Global*, *Chambers & Partners* and *IFLR1000*.

Sokol graduated in Law at the University of Tirana in 1996 and is admitted to practice in Albania and Kosovo. He is also an arbiter listed in the roster of the American Chamber of Commerce of Kosovo.

He is fluent in English and Italian.

Delvina Nallbani
Boga & Associates
Nene Tereza Str. Entry 30
No. 5 Pristina
Kosovo

Tel: +381 38 223 152
Email: dnallbani@bogalaw.com
URL: www.bogalaw.com

Delvina is a Senior Associate at Boga & Associates, which she joined in 2012.

Her practice is mainly focused on providing legal advice to clients on a wide range of corporate, business and banking matters. She also provides assistance in advising investors on a number of transactions, including mergers and acquisitions, and privatisations.

Delvina graduated in Law at the University of Zagreb, and is a member of the Kosovo Bar Association

She is fluent in Croatian and English.

BOGA & ASSOCIATES

LEGAL • TAX • ACCOUNTING

Boga & Associates, established in 1994, has emerged as one of the premier law firms in Albania, earning a reputation for providing the highest quality of legal, tax and accounting services to its clients. The firm also operates in Kosovo (Pristina) offering a full range of services. Until May 2007, the firm was a member firm of KPMG International and the Senior Partner/Managing Partner, Mr. Genc Boga, was also the Senior Partner/Managing Partner of KPMG Albania.

The firm's particularity is linked to the multidisciplinary services it provides to its clients, through an uncompromising commitment to excellence. Apart from the widely consolidated legal practice, the firm also offers the highest standards of expertise in tax and accounting services, with keen sensitivity to the rapid changes in the Albanian and Kosovo business environment.

The firm delivers services to leading clients in major industries, banks and financial institutions, as well as to companies engaged in insurance, construction, energy and utilities, entertainment and media, mining, oil and gas, professional services, real estate, technology, telecommunications, tourism, transport, infrastructure and consumer goods.

The firm is continuously ranked as a "top tier firm" by *The Legal 500*, by *Chambers and Partners* for Corporate/Commercial, Dispute Resolution, Projects, Intellectual Property, Real Estate, as well as by *IFLR* in Financial and Corporate Law. The firm is praised by clients and peers as a *"law firm with high-calibre expertise"*, *"the market-leading practice"*, *"a unique legal know-how"*, distinguished *"among the elite in Albania"* and described as *"accessible, responsive and wise"*.

Current titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- 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 Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

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

www.iclg.com