ICLG

The International Comparative Legal Guide to:

Cybersecurity 2019

2nd Edition

A practical cross-border insight into cybersecurity work

Published by Global Legal Group, with contributions from:

Advokatfirmaet Thommessen AS
Allen & Overy LLP
Angara Abello Concepcion Regala & Cruz Law Offices
Bagus Enrico & Partners
Boga & Associates
BTG Legal
Christopher & Lee Ong
Cliffe Dekker Hofmeyr Inc
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Eversheds Sutherland
Ferchiou & Associés
Gikera & Vadgama Advocates
Gouveia Pereira, Costa Freitas & Associados, S.P. R.L.
JIPYONG LLC
King & Wood Mallesons
Latham & Watkins LLP
Lee, Tsai & Partners Attorneys-at-Law
LT42 – The Legal Tech Company
Maples and Calder
Mori Hamada & Matsumoto
Niederer Kraft Frey Ltd.
Nyman Gibson Miralis
Pearl Cohen Zedek Latzer Baratz
R&T Asia (Thailand) Limited
Rajah & Tann Singapore LLP
Simmons & Simmons LLP
Siqueira Castro Advogados
Stehlin & Associes
Synch
Templars
USCOV | Attorneys at Law

glg
global legal group

glg
global legal group

Contributing Editors
Nigel Parker & Alexandra Rendell, Allen & Overy LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Editor
Sam Friend

Senior Editors
Suzie Levy
Caroline Collingwood

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 2018

ISBN 978-1-912509-38-6
ISSN 2515-4206

Strategic Partners

General Chapters:

1 **The Regulators Have Spoken – Nine Lessons To Help Protect Your Business –** Nigel Parker & Alexandra Rendell, Allen & Overy LLP 1

2 **Cybersecurity and Digital Health: *Diabolus ex Machina*? –** Paolo Caldato & David Fitzpatrick, Simmons & Simmons LLP 5

3 **Ten Questions to Ask Before Launching a Bug Bounty Program –** Serrin Turner & Alexander E. Reicher, Latham & Watkins LLP 12

Country Question and Answer Chapters:

4	**Albania**	Boga & Associates: Genc Boga & Eno Muja	17
5	**Australia**	Nyman Gibson Miralis: Phillip Gibson & Dennis Miralis	22
6	**Brazil**	Siqueira Castro – Advogados: Daniel Pitanga Bastos De Souza	28
7	**China**	King & Wood Mallesons: Susan Ning & Han Wu	33
8	**Denmark**	Synch: Niels Dahl-Nielsen & Daniel Kiil	40
9	**England & Wales**	Allen & Overy LLP: Nigel Parker & Alexandra Rendell	46
10	**France**	Stehlin & Associes: Frederic Lecomte & Victoire Redreau-Metadier	54
11	**Germany**	Eversheds Sutherland: Dr. Alexander Niethammer & Steffen Morawietz	61
12	**India**	BTG Legal: Prashant Mara & Devina Deshpande	67
13	**Indonesia**	Bagus Enrico & Partners: Enrico Iskandar & Bimo Harimahesa	75
14	**Ireland**	Maples and Calder: Kevin Harnett & Victor Timon	82
15	**Israel**	Pearl Cohen Zedek Latzer Baratz: Haim Ravia & Dotan Hammer	90
16	**Italy**	LT42 – The Legal Tech Company: Giuseppe Vaciago & Marco Tullio Giordano	97
17	**Japan**	Mori Hamada & Matsumoto: Hiromi Hayashi	104
18	**Kenya**	Gikera & Vadgama Advocates: Hazel Okoth & Stella Ojango	112
19	**Korea**	JIPYONG LLC: Seung Soo Choi & Seungmin Jasmine Jung	118
20	**Kosovo**	Boga & Associates: Genc Boga & Delvina Nallbani	124
21	**Malaysia**	Christopher & Lee Ong: Deepak Pillai & Yong Shih Han	130
22	**Mexico**	Creel, García-Cuéllar, Aiza y Enríquez, S.C.: Begoña Cancino	139
23	**Nigeria**	Templars: Ijeoma Uju & Ijeamaka Nzekwe	145
24	**Norway**	Advokatfirmaet Thommessen AS: Christopher Sparre-Enger Clausen & Uros Tosinovic	151
25	**Philippines**	Angara Abello Concepcion Regala & Cruz Law Offices: Leland R. Villadolid Jr. & Arianne T. Ferrer	158
26	**Portugal**	Gouveia Pereira, Costa Freitas & Associados, S.P. R.L.: Miguel Duarte Santos & Sofia Gouveia Pereira	166
27	**Romania**	USCOV | Attorneys at Law: Silvia Uscov & Tudor Pasat	172
28	**Singapore**	Rajah & Tann Singapore LLP: Rajesh Sreenivasan & Michael Chen	178
29	**South Africa**	Cliffe Dekker Hofmeyr Inc: Fatima Ameer-Mia & Christoff Pienaar	185
30	**Sweden**	Synch: Anders Hellström & Erik Myrberg	192
31	**Switzerland**	Niederer Kraft Frey Ltd.: Dr. András Gurovits & Clara-Ann Gordon	199
32	**Taiwan**	Lee, Tsai & Partners Attorneys-at-Law: Sean Yu-Shao Liu & Sophia Ming-Chia Tsai	206
33	**Thailand**	R&T Asia (Thailand) Limited: Saroj Jongsaritwang & Sui Lin Teoh	213
34	**Tunisia**	Ferchiou & Associés: Amina Larbi & Rym Ferchiou	219
35	**USA**	Allen & Overy LLP: Keren Livneh & Jacob Reed	225

Albania

Genc Boga

Eno Muja

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:

The content of the following offences can be found in various articles of the "Criminal Code of the Republic of Albania", even though the latter does not provide a literal denomination of them.

Hacking (i.e. unauthorised access)

Hacking constitutes a criminal offence in the Albanian jurisdiction. Article 192/b/1 of the "Criminal Code of the Republic of Albania" provides that unauthorised access or excess of authorisation to a computer system or part of it, through violation of security measures, is punishable by a fine or imprisonment for up to three years. According to the Final Report of the General Prosecutor on the state of criminality for the year 2017, 11 cases have been recorded by the Prosecution body, two of which have ended with the sentencing of the accused, but no further details have been given.

Denial-of-service attacks

Article 293/c/1 of the "Criminal Code of the Republic of Albania" provides that the creation of serious and unauthorised obstacles to harm the function of a computer system, through insertion, damage, deformation, change or deletion of data, is punishable with imprisonment for three to seven years. According to the Final Report of the General Prosecutor on the state of criminality for the year 2017, four cases have been recorded by the Prosecution body, but no details have been given on the cases.

Phishing

Article 143/b of the "Criminal Code of the Republic of Albania" states that adding, modifying or deleting computer data or interfering in the functioning of a computer system, with the intention of ensuring for oneself or for third parties, through fraud, unfair economic benefits or causing a third party reduction of wealth, is punishable by imprisonment for six months to six years and a fine from 60,000 Leke to 600,000 Leke. According to the Final Report of the General Prosecutor on the state of criminality for the year 2017, 73 cases have been recorded by the Prosecution body, but no details have been given on the cases.

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

Article 293/b of the "Criminal Code of the Republic of Albania" provides that damage, deformation, change or unauthorised deletion of computer data is punishable by imprisonment for six months to three years. According to the Final Report of the General Prosecutor on the state of criminality for the year 2017, 33 cases have been recorded by the Prosecution body, four of which have ended with the sentencing of the accused, but no details have been given on the cases.

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

Article 293/ç of the "Criminal Code of the Republic of Albania" provides that manufacturing, keeping, selling, giving for use, distribution or any other action to place at disposal any equipment, including a computer program, computer password, access code or any other similar data, created or adapted for breaching a computer system or a part of it, with the aim of committing a criminal act, as provided in articles 192/b, 293/a, 293/b and 293/c of the "Criminal Code of the Republic of Albania", is punishable by imprisonment for six months to five years. According to the Final Report of the General Prosecutor on the state of criminality for the year 2017, one case has been recorded by the Prosecution body.

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

Even though the "Criminal Code of the Republic of Albania" does not explicitly mention or provide an article dedicated to identity theft, article 186/a states that modifying, deleting, or omitting computer data, without the right to do so, in order to create false data, with the intention of presenting and using them as authentic, even though the created data is directly readable or understandable, are all punishable by imprisonment for six months to six years. According to the Final Report of the General Prosecutor on the state of criminality for the year 2017, 16 cases have been recorded by the Prosecution body, one of which has ended with the sentencing of the accused, but no details have been given.

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

Article 186/a/2 of the "Criminal Code of the Republic of Albania" provides that when the aforementioned criminal act, as described in the provision of identity theft above, is done by the person responsible for safekeeping and administering the computer data in cooperation more than once, or has brought forth grave consequences for the public interest, is punishable by imprisonment for three to 10 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

Article 293/b/2 of the "Criminal Code of the Republic of Albania" provides that damage, deformation, change or unauthorised deletion of computer data, when done in regard to military computer data,

national security, public order, civil protection, and healthcare or in any other computer data with public importance, is punishable by imprisonment for three to 10 years.

Failure by an organisation to implement cybersecurity measures

In virtue of Law No. 2/2017, "On cybersecurity", failure by an organisation to implement cybersecurity measures does not constitute a criminal offence. Article 21 of the Law "On cybersecurity" provides that failure to implement cybersecurity measures is considered an administrative violation and is punishable by a fine.

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

The Convention "On cyber crime", ratified in Albania on 25.04.2002 through Law No. 8888, provides, in article 22, that Member States of the Convention must determine the jurisdiction in cases when a cyber crime is committed in their territory or by a citizen of that state. Article 6/2 of the "Criminal Code of the Republic of Albania" provides that Albanian law is also applicable to Albanian citizens who commit a crime in the territory of another state, when the crime is at the same time punishable and as long as there is not any final decision by any foreign court for that crime. Also, article 7/a of the "Criminal Code of the Republic of Albania" states that the criminal law of the Republic of Albania is also applicable to foreign citizens who have committed a criminal act outside the territory of the Republic of Albania for which special laws or international agreements, of which the Republic of Albania is a part of, determine the application of the Albanian criminal legislation.

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?

Article 48 of the "Criminal Code of the Republic of Albania" provides mitigating circumstances for any penalty. These circumstances include, but are not limited to: a) when the criminal act is driven by motives of positive moral and social value; b) when the criminal act is done under the influence of psychic shock caused by provocation or unfair actions of the victim or any other person; c) when the criminal act is done under the influence or unfair instruction of a superior; ç) when the person responsible for the criminal act shows deep repentance; d) when the person has replaced the damage caused by the criminal act or has actively helped to erase or minimise the consequences of the criminal act; dh) when the person presents him/herself before the competent bodies after committing the criminal act; and e) when the relations between the person who has committed the criminal act and the person who has suffered the consequences of the criminal act have returned to normal.

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.

Article 74/a of the "Criminal Code of the Republic of Albania" states that distributing or offering to the public through computer systems materials that deny, minimise, or significantly approve or justify acts which constitute genocide or crimes against humanity is punishable by imprisonment for three to six years. Also, article 84/a of the "Criminal Code of the Republic of Albania" provides that serious threats to kill or seriously injure a person through computer systems because of ethnicity, nationality, race or religion are punishable by a fine or imprisonment for up to three years. Article 119/a of the "Criminal Code of the Republic of Albania" states that offering or distributing to the public through computer systems materials with racist or xenophobic content constitutes an administrative violation and is punishable by a fine or imprisonment for up to two years. Article 119/b of the "Criminal Code of the Republic of Albania" provides that a public insult involving ethnicity, nationality, race or religion through a computer system constitutes an administrative violation and is punishable by a fine or imprisonment for up to two years.

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.

1. The Convention "On cyber crime" ratified in Albania on 25.04.2002 with Law No. 8888.
2. Law No. 7895, dated 27.01.1995, "Criminal Code of the Republic of Albania", as amended.
3. Law No. 2/2017 "On cybersecurity".
4. Law No. 9918, dated 19.05.2008, "On electronic communications in the Republic of Albania", as amended.
5. Law No. 9887, dated 10.03.2008, "On protection of personal data", as amended.
6. Law No. 8457, dated 11.02.1999, "On classified information 'Secrets of State'".
7. Law No. 9880, dated 25.02.2008, "On electronic signatures", as amended.
8. The Decision of Council of Ministers No. 141, dated 22.02.2017, "On organising and functioning of the national authority for electronic certification and cybersecurity".

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

Article 8 of the Law "On cybersecurity" specifies that operators of critical infrastructure of information are obliged to implement the requirements of safety measures, and to also document their implementation. Article 9/3 of the Law "On cybersecurity" provides that the Responsible Authority for Electronic Certification and Cybersecurity (herein the "Authority") determines, through a regulation, the content and method of documenting the safety measures. To the best of our knowledge, no such regulation exists.

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.

Article 9 of the Law "On cybersecurity" provides a list of safety measures and divides them into two groups: organisational measures;

and technical measures. As specified above, the Authority determines, through a regulation, the content and method of documenting the safety measures. To date, no such regulation exists.

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.

To the best of our knowledge, no such conflict of laws issues arise.

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.

Article 11 of the Law "On cybersecurity" provides that operators of critical infrastructure of information and operators of important infrastructure of information are obliged to report immediately to the Authority after they discover any Incidents. The Authority determines, through a specific regulation, the types and categories of Incidents regarding cybersecurity. In the case of Incidents at constitutional institutions (for example, those of security and defence), the Authority reports immediately to the directors of these institutions. In addition, article 12 provides the type of information which is kept and administered in the electronic register of the Authority: data regarding the Incident report; data on identification of the system in which the Incident happened; data on the source of the Incident; and the procedure for solving the Incident and its result. Article 14 states that the Authority shall maintain full confidentiality of the data collected during the process of solving the Incident.

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?

Organisations are required to share information related to Incidents or potential Incidents, with contact points determined by the operators of critical infrastructure of information or the operators of important infrastructure of information. The Authority has also provided a standard form to be completed in case of Incidents.

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.

To the best of our knowledge and after carefully reviewing the legislation, there are no provisions as regards this situation.

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 responses to questions 2.5 to 2.7 do not change regardless of the information included.

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

Article 8 of the Law "On cybersecurity" provides that operators of critical infrastructure of information and operators of important infrastructure of information are obliged to implement the safety measures and also document their implementation. Furthermore, the aforementioned operators are obliged to implement the requirements of the safety measures during the establishment of infrastructure.

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

Article 22 of the Law "On cybersecurity" states that in case of non-compliance with the requirements specified in the law, the Authority issues fines from 20,000 Leke to 800,000 Leke.

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

To the best of our knowledge there are no examples of enforcement action taken in cases of non-compliance with the abovementioned requirements.

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 not any difference as regards the variety of measures taken across different business sectors, because the Law "On cybersecurity" is applied the same regardless of the business sector.

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?

The Law "On cybersecurity" is the only one governing with regard to cybersecurity for all organisations, private or public, in the Republic of Albania.

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?

The Law "On cybersecurity" does not elaborate on this point, but nevertheless this is a matter of regulation inside the company.

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?

To the best of our knowledge, there is no obligation to fulfil these requirements. The Authority shall draft, approve and publish the necessary regulations to complete the legislative frame for cybersecurity within 12 months of the date of the law's approval.

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)?

The Law "On cybersecurity", even though it does not clearly mention companies, provides the obligation to report to the competent authorities. However, the "Code of Criminal Procedure of the Republic of Albania" demands disclosure when legally asked by the Prosecution, be it through an order or a court decision.

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

To the best of our knowledge, companies are not subject to any other specific requirements under Applicable Laws in relation to cybersecurity.

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.

For a civil action to be brought in relation to any Incident, it is necessary to provide the element of damage caused by a person committing an illegal action and evidence the causality of this action. It is also necessary to identify the source or the person responsible for the Incident.

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

To the best of our knowledge, there are no specific examples of cases brought in relation to Incidents.

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

The Law "On cybersecurity" does not provide any specifics in this regard, but there is potential liability in tort in relation to an Incident, in virtue of the "Civil Code of the Republic of Albania", as specified above.

6 Insurance

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

To the best of our knowledge, organisations are not prohibited from taking out insurance against Incidents.

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 regulatory limitations to insurance coverage against specific types of loss, such as business interruption, etc.

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?

Article 9 of the Law "On cybersecurity" states that responsible bodies should take the necessary measures to manage and monitor the safety of human resources and people's access.

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?

To the best of our knowledge and after carefully reviewing the current Albanian legislation on the matter, there are no prohibitions in this regard.

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.

Structures for cyber crime at the County Directory Police and General County Directory Police are responsible for investigating any crimes related to cybersecurity. In addition, the State Police has made available to the public a website (http://www.policia.al/denonco/) where every person can report in real-time any criminal act related to cyber crimes. The Authority is also responsible for investigating any reported crimes related to cybersecurity.

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?

To the best of our knowledge, there are no requirements under Applicable Laws for organisations to implement backdoors in their IT systems.

Genc Boga
Boga & Associates
40/3 Ibrahim Rugova Str.
1019 Tirana
Albania

Tel: +355 4 2251 050
Email: gboga@bogalaw.com
URL: www.bogalaw.com

Genc Boga is the founder and Managing Partner of Boga & Associates, which operates in both jurisdictions of Albania and Kosovo. Mr. Boga's fields of expertise include business and company law, concession law, energy law, corporate law, banking and finance, taxation, litigation, competition law, real estate, environment protection law, etc.

Mr. Boga has solid expertise as an advisor to banks, financial institutions and international investors operating in major projects in the energy, infrastructure and real estate sectors. Thanks to his experience, Boga & Associates is retained as a legal advisor on a regular basis by the most important financial institutions and foreign investors.

He regularly advises the EBRD, IFC and the World Bank on various investment projects in Albania and Kosovo.

Mr. Boga is continuously ranked as a leading lawyer in Albania by major legal directories: *Chambers Global*; *Chambers Europe*; *The Legal 500*; and *IFLR 1000*.

He is fluent in English, French and Italian.

Eno Muja
Boga & Associates
40/3 Ibrahim Rugova Str.
1019 Tirana
Albania

Tel: +355 4 2251 050
Email: emuja@bogalaw.com
URL: www.bogalaw.com

Eno Muja is an Associate at Boga & Associates.

His core practice area is litigation overarching a wide range of legal issues in Albania, mainly related to private law.

Eno represents international clients in district courts and appeal courts, in cases dealing with real estate, employment law and all sorts of other commercial/corporate disputes.

Additionally, he has also covered practice areas in IP Law and Data Protection.

Eno graduated in Law at the State University of Tirana and obtained a Master of Science degree focused on Private Law in 2014. He has been a member of the Albanian Bar Association since 2016.

Eno is fluent in English, Italian, and French.

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 major directories: *Chambers Europe*; *The Legal 500*; and *IFLR 1000*.

Other 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
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- 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
- 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