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:

Country Question and Answer Chapters:

Germany

Dr. Alexander Niethammer

Eversheds Sutherland

Steffen Morawietz

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:

All of the following activities constitute a criminal offence in Germany.

Hacking (i.e. unauthorised access)

Hacking constitutes a criminal offence according to Sec. 202a of the German Criminal Code (so-called "unauthorised obtaining of data"). According to this provision, whosoever unlawfully obtains data for himself, or another, that was not intended for him and was especially protected against unauthorised access, if he has circumvented the protection, shall be liable to imprisonment not exceeding three years or a fine.

Denial-of-service attacks

Denial-of-service attacks constitute a criminal offence according to Sec. 303b of the German Criminal Code (so-called "computer sabotage"). According to this provision, whosoever interferes with data processing operations which are of substantial importance to another by deleting, suppressing, rendering unusable or altering data, or by entering or transmitting data with the intention of causing damage to another, shall be liable to imprisonment for up to three years or a fine. The same applies to destroying, damaging, rendering unusable, removing or altering a data processing system or data carrier. Also, it is important to note that the sole attempt is punishable and if the data processing operation is of substantial importance for another's business or enterprise, or a public authority, the penalty can be imprisonment for up to five years or a fine.

Phishing

Phishing can constitute two different criminal offences. The unlawful interception of data by technical means from a non-public data processing facility constitutes a criminal offence according to Sec. 202b of the German Criminal Code and is punishable with imprisonment for up to two years or a fine. The *use* of such data with the intent of obtaining an unlawful material benefit would constitute a criminal offence under Sec. 263a of the German Criminal Code (so-called "computer fraud") and is punishable with imprisonment for up to five years or a fine.

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

Infection of IT systems with malware constitutes a criminal offence according to Sec. 303b of the German Criminal Code (so-called "computer sabotage"). According to this provision, whosoever interferes with data processing operations which are of substantial importance to another by deleting, suppressing, rendering unusable or altering data, or by entering or transmitting data with the intention of causing damage to another, shall be liable to imprisonment for up to three years or a fine. The same applies to destroying, damaging, rendering unusable, removing or altering a data processing system or data carrier. Also, it is important to note that the sole attempt is punishable and if the data processing operation is of substantial importance to another's business or enterprise, or a public authority, the penalty can be imprisonment for up to five years or a fine.

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

The sole possession of hardware, software or other tools which can be used to commit cybercrime can constitute a criminal offence according to Sec. 202c of the German Criminal Code. According to this provision, the preparation of the commission of an unauthorised obtaining of data or phishing by producing, acquiring for himself or another, selling, supplying to another, disseminating or making otherwise accessible software for the purpose of the commission of such an offence shall be liable to imprisonment for up to one year or a fine. In case of a use of such instruments, the same principles as set forth above with respect to "Hacking" apply.

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

Identity theft can constitute various criminal offences, depending on how the offender obtains access to the identity data. This can either be done by phishing methods, which would constitute a criminal offence under Sec. 202b of the German Criminal Code as set forth above with respect to "Phishing", or by use of such identity data for fraudulent purposes, which could constitute a criminal offence under Sec. 263 of the German Criminal Code (fraud) or Sec. 263a of the German Criminal Code (computer fraud); both are subject to imprisonment for up to 10 years.

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

Electronic theft only constitutes a criminal offence under the preconditions of Sec. 202a of the German Criminal Code. Therefore, the affected data must be especially protected against unauthorised access. Usually, this is not the case when a current or former employee breaches confidence, as the employee has authorised access

to the data. If this is not the case and the employee circumvents the protection, this would constitute the criminal offence of "phishing". The above-mentioned principles would apply.

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

Under German criminal law, some other activities in connection with the above-mentioned crimes constitute criminal offences. These are: (i) *preparing* of an unauthorised obtaining or interception of data, Sec. 202c of the German Criminal Code; (ii) handling of stolen data, Sec. 202d of the German Criminal Code; (iii) violation of postal and telecommunications secrets, Sec. 206 of the German Criminal Code; (iv) computer sabotage, Sec. 303b of the German Criminal Code; (v) certain types of violation of the EU General Data Protection Regulation with the intention of enrichment or to harm someone, Art. 84 of the General Data Protection Regulation and Sec. 42 of the German Federal Data Protection Act; and (vi) falsification of digital evidence, Sec. 269 *et seq.* of the German Criminal Code.

Failure by an organisation to implement cybersecurity measures

The failure of an organisation to implement cybersecurity measures does not constitute a criminal but an administrative offence, and the organisation would be subject to civil liability in case of negligence. The financial penalty can be up to 10 million EUR or 2% of the company's annual turnover. The civil liability depends on the damage which occurred due to the organisation's failure and is basically not limited.

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

The above-mentioned offences have no specific extraterritorial application. However, the application of the German Criminal Code depends on the "place of the offence". According to Sec. 9 of the German Criminal Code, an offence is deemed to have been committed in every place where the offender acted or in which the result occurs or should have occurred according to the intention of the offender. Therefore, the above-mentioned offences will be applicable both if the offender acted in the territory of Germany and in case the offence affects IT systems which are situated or used for services provided in Germany where the offender acted from outside Germany.

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?

Yes, as a general principle, under German law, positive behaviour after a violation of a statutory provision as well as compensation for the occurred damage affect the level of penalties. However, this is at the sole discretion of the court.

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.

No, this is not applicable in our jurisdiction.

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.

Cybersecurity is governed by several Acts in Germany. The main law relating to cybersecurity is the German IT Security Act (*IT-Sicherheitsgesetz*) of 25 July 2015, which amended a number of laws, in particular the German Telemedia Act (*Telemediengesetz*), the German Telecommunications Act (*Telekommunikationsgesetz*), the EU General Data Protection Regulation (*Datenschutz-Grundverordnung*), the German Federal Data Protection Act (*Bundesdatenschutzgesetz*) and the Act on the Federal Office for Information Security (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik*). Besides this, parts of cybersecurity are governed by the Banking Act (*Kreditwesengesetz*) and Securities Trading Act (*Wertpapierhandelsgesetz*). Besides this formal legislation, there are a few important informal provisions with respect to IT security in Germany. These are the BSI Basic IT Protection catalogues which are developed by the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik – BSI*), the Common Criteria for Information Technology Security Evaluation, standardised as ISO/IEC 15408, and the Control Objectives for Information and Related Technology (COBIT).

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.

Yes, the Act on the Federal Office for Information Security provides for specific obligations for providers of critical infrastructure. The law defines the following sectors as critical infrastructure:

- Energy.
- IT and Telecommunications.
- Transport and Traffic.
- Health.
- Water.
- Nutrition.
- Finance and Insurance.

However, not all companies acting in the above-mentioned sectors are subject to the regulations regarding critical infrastructure. These apply only *vis-à-vis* companies which are of great importance to the functioning of the community or which would cause a threat of public safety when having a supply shortfall.

Even though the Act on the Federal Office for Information Security provides for the obligation of providers of critical infrastructure to provide reasonable organisational and technical precautions to prevent disruption of the availability, integrity, authenticity and confidentiality of their information technology systems, the specific duties are not specified by the Act but are subject to guidelines on IT security set out by industry associations and approved by the Federal Office for Information Security.

The Network and Information Systems Directive has been implemented with effect from 30 June 2017.

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.

Yes, German and European law provides for several obligations for organisations to take measures to monitor, detect, prevent and mitigate Incidents.

In detail:

- According to Sec. 13, subsec. 7 of the Telemedia Act, telemedia providers are obliged to ensure that unauthorised access to related data is not possible. A telemedia provider in the Telemedia Act means, e.g., each operator of a website. The Telemedia Act does not provide details for measures that have to be taken by the provider. Specific requirements are, however, developed by the competent data protection authorities, e.g., with respect to the prevention of unauthorised access to websites, the data protection authorities request a SSL encryption of the related data.
- According to Sec. 109 of the German Telecommunications Act, providers of public telecommunications have to implement necessary technical measures to prevent phishing of personal data. Besides this, providers of public telecommunications are obliged to appoint a security officer and develop an adequate IT security model.
- Providers of several financial products are obliged to develop an IT-specific risk management (Sec. 25a of the German Banking Act (*Kreditwesengesetz*), Sec. 33 of the German Securities Trading Act (*Wertpapierhandelsgesetz*)).
- According to Art. 5 para. 1 (f) and Art. 32 of the General Data Protection Regulation, organisations are obliged to process personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

This includes in particular:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical Incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

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.

Such specific conflicts may arise with foreign laws with exterritorial reach.

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.

Yes, there are specific reporting obligations with respect to Incidents under German law.

In detail:

- There is a general obligation to notify security breaches to the competent data protection authority. This applies to any kind of personal data. An exception applies where the security breach is unlikely to result in a high risk to the rights and freedoms of the data subject (Art. 33 of the EU General Data Protection Regulation).

  The report must be made without undue delay and not later than 72 hours after having become aware of the breach and has to contain a description of the Incident, an indication of the category of the affected data, the concerned data subjects and a detailed description of the measures taken to remedy or mitigate negative effects. The notification to the competent data protection authority must also describe possible harmful consequences of the unlawful access and measures taken by the body. The name and contact details of the data protection officer have to be provided as well.
- In case of a breach of critical infrastructure as defined in the Act on the Federal Office for Information Security (see above under question 2.2), the provider must notify the Federal Office for Information Security of any significant disruption to the availability, integrity and confidentiality of their information technology systems, components or processes which might lead to a breakdown or malfunction of the affected infrastructure.
- Providers of public telecommunications networks or services are obliged to report any IT breach to the Federal Network Agency. The report, which must be made immediately, has to contain a description of the Incident, an indication of the category of the affected data, the concerned data subjects and a detailed description of the measures taken to remedy or mitigate negative effects.

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?

Yes, there is no prohibition of such voluntary reports as long as possible (confidentiality) rights of third parties are safeguarded.

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.

Yes, in case of a security breach which creates a notification obligation (see above under question 2.5), the data subject must be notified as soon as (i) appropriate measures have been taken to secure the data or have not been carried out without undue delay, and (ii) a criminal enforcement is not/no longer at risk. The notification to the data subjects must describe the nature of the unlawful access and include recommendations for measures to minimise possible harm. Where notifying the data subjects would require unreasonable efforts, such notification may be replaced by a public communication or similar measure whereby the data subjects are informed in an equally effective manner (Art. 34 General Data Protection Regulation). This obligation of notification applies provided the Incident is likely to result in a high risk to the rights and freedoms of the data subject. Further exceptions apply under Art. 34, para. 3 of the General Data Protection Regulation and Sec. 29 of the Federal Data Protection Act.

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?

No, none of these scenarios would change the responses to questions 2.5 to 2.7.

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

The requirements identified under questions 2.3 to 2.7 are enforced by the Federal Office for Information Security, competent Data Protection Authorities and the Federal Network Agency.

In detail:

- The Federal Office for Information Security is the main authority with respect to cybersecurity in Germany. This authority should be the main contact regarding questions about preventive security measures and is responsible for receiving notifications about security breaches with respect to critical infrastructures.
- Data Protection Authorities enforce all relevant data protection laws. In Germany, each federal state has a separate Data Protection Authority.
- The Federal Network Agency enforces the telecommunications-related laws and is responsible for receiving notifications about security breaches with respect to telecommunications networks and services.

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

Under the German IT Security Act, non-compliance may be subject to administrative fines of up to 100,000 EUR. Non-compliance with the mentioned requirements under the General Data Protection Regulation is subject to fines up to 10 million EUR or 2% of the worldwide annual turnover, whichever is higher.

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

Up to now, no publicly known enforcement actions have been taken by the competent authorities in cases of non-compliance with cybersecurity requirements. The reason for this is that most of the relevant laws are rather new and the competent authorities are currently trying to develop a joint position with the industry. However, this might change in the future.

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.

The market practice with respect to information security in Germany mainly depends on the security relevance of the concrete business; in particular, whether the sector is considered as a sector which is related to critical infrastructures and whether the business processes sensitive personal data or not. However, there are no known sector-specific deviations from the strict legal requirements.

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?

Yes, in detail:

- Providers of certain financial products are obliged to develop an IT-specific risk management (Sec. 25a of the German Banking Act (*Kreditwesengesetz*), Sec. 33 of the German Securities Trading Act (*Wertpapierhandelsgesetz*)).
- According to Sec. 109 of the German Telecommunications Act, providers of public telecommunications have to implement the necessary technical measures to prevent phishing of personal data. Besides this, providers of public telecommunications are obliged to appoint a security officer and develop an adequate IT security model.

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?

Yes, such failure may lead to a breach of directors' duties.

According to Sec. 130 of the German Administrative Offences Act (*Ordnungswidrigkeitengesetz – OWiG*), the owner or management of a company commits a misdemeanour if:

- it omits purposefully or negligently to appropriately control the company; and
- if a crime or misdemeanour was committed that could have been avoided or significantly impeded by exercising such control.

The obligation to control also includes the obligation to diligently select and monitor supervising personnel, active monitoring of the development of legal and technical standards, random inspections, and enforcement of implementation measures, etc. The owner or management of a company is obligated to organise the company in a manner that allows the company to comply with the law. Consequently, failures to prevent, mitigate, manage or respond to an Incident can constitute a breach of directors' duties if the directors failed to implement the appropriate measures to avoid such occurrences.

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 are no general obligations, so far, to either designate a CISO, establish a written Incident response plan or policy, or conduct periodic cyber risk assessments. However, according to Art. 32 of the General Data Protection Regulation, such measures can be required in order to ensure appropriate IT security measures. Companies shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. In particular, companies shall implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of data processing. This has to be therefore assessed on a case-by-case basis.

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)?

Notification requirements generally exist solely with respect to security breaches (see question 2.5 above). However, with respect to publicly listed companies, sole cybersecurity risks without an Incident having occurred may trigger the obligation to disclose the cybersecurity risk in an *ad hoc* notification if the risk is likely to have an impact on the company's stock market price.

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

Companies are obliged to implement an IT security model. However, there are no detailed statutory provisions regarding such models.

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.

The civil liability of a company depends on whether damage has occurred due to the organisation's failure to implement an appropriate IT security model. In this case, any individual or other company which suffered material damage can take civil actions against the company which is responsible for the Incident. This liability is basically not limited, but can be covered by insurance.

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

The case law on Incidents in Germany is very rare due to the lack of the possibility of class actions in Germany.

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

Yes, civil liability in tort depends on the damage which occurred due to the organisation's failure and is basically not limited.

6 Insurance

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

Yes, organisations are permitted to take out insurance against Incidents and are common in Germany.

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?

No, there are no regulatory limitations to insurance coverage against any type of loss.

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?

(a) Yes, the monitoring of employees is only permissible in specific cases, e.g., in case of definite suspicion. Comprehensive monitoring measures would not be admissible. In case of works-council representation, the monitoring of employees needs to be generally agreed in a works-council agreement.

(b) There is no specific statutory obligation for employees to report such risks to their employer. However, such obligations should be imposed on the employees by the employer's internal policies (e.g., whistle-blowing policies).

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?

No, there are no Applicable Laws that may prohibit or limit the reporting of the above.

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.

Depending on the type of authority (e.g., Public Prosecutor, Federal Office for Information Security, Data Protection Authority), the enforcement powers vary. However, all authorities have the power to carry out on-site investigations including accessing IT systems.

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?

No; so far, there is no such obligation. However, the German legislator is currently debating such an obligation with respect to social media and instant messaging accounts. It is likely that such a law will come into force in 2018.

Dr. Alexander Niethammer
Eversheds Sutherland
Brienner Str. 12
80333 Munich
Germany

Tel: *+49 89 545 65 318*
Email: *alexanderniethammer@eversheds-sutherland.de*
URL: *www.eversheds-sutherland.de*

Alexander Niethammer is a Partner in the Munich office of Eversheds Sutherland and heads the Company Commercial Practice Group in Germany. He specialises in complex IT transactions, cybersecurity and data protection. Alexander has advised, for over 14 years, many Fortune 100 companies from the IT, DI, Consumer and Financial sectors on global projects.

Alexander has a dual legal qualification an as attorney-at-law in New York (USA) as well as in Germany.

Alexander was recently named by the International Law Office (ILO) as the exclusive recipient of the prestigious "Client Choice Award" 2016 as Germany's best IT & Internet counsel.

Steffen Morawietz
Eversheds Sutherland
Brienner Str. 12
80333 Munich
Germany

Tel: *+49 89 545 65 262*
Email: *steffenmorawietz@eversheds-sutherland.de*
URL: *www.eversheds-sutherland.de*

Steffen Morawietz is an Associate in the IT/IP practice at Eversheds Sutherland in Munich. His activities include providing legal advice to international companies in the areas of IT law and data protection. Steffen's advice focuses on companies in the e-commerce sector, in particular with regard to data protection, cybersecurity and consumer protection requirements, contract drafting and distribution law matters. He mainly advises international and national clients from the media, sports and consumer goods industries out of court as well as in court, in particular with regard to interim legal protection. Moreover, Steffen is appointed as a lecturer in civil and public law at Ludwig Maximilians University of Munich.

EVERSHEDS SUTHERLAND

Eversheds Sutherland is a one of the leading legal service providers in the world. Eversheds Sutherland represents the combination of two firms with a shared culture and commitment to client service excellence. We are each known for our commercial awareness and industry knowledge and for providing innovative and tailored solutions for every client.

With 66 offices in 32 countries and more than 2,400 lawyers, we partner with many of the most dynamic and successful business organisations across Africa, Asia, Europe, the Middle East and the United States, to address their most critical challenges, supporting their legal needs and unlocking their global ambitions.

Our international IT team frequently works for major corporate and public clients across the globe, and also acts for some of the world-leading IT suppliers. Our cybersecurity practice spans the full range of data protection, cyber and information security law topics.

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