Das neue IT-Sicherheitsgesetz – Erweiterte Sicherungs- und Berichtspflichten für Betreiber Kritischer Infrastrukturen

Deutschland gehört zu den führenden Industrie- und Technologienationen. Einer der Pfeiler dieser Führungsrolle ist das gut ausgebaute Telekommunikationsnetz und die darauf aufbauende enge Vernetzung aller Infrastrukturbereiche. Ständig steigende Zahlen von Angriffen auf die IT-Systeme von Unternehmen und öffentlicher Hand einerseits und ein gewachsenes Bewusstsein der möglichen schwerwiegenden Folgen von Störungen der IT-Infrastruktur für Wirtschaft und Gesellschaft andererseits, haben den deutschen Gesetzgeber veranlasst, neue regulatorische Maßnahmen zur Stärkung der IT-Sicherheit zu ergreifen.

In diesem Zuge hat der Deutsche Bundestag am 12. Juni 2015 das IT-Sicherheitsgesetz verabschiedet.[1] Von den verschiedenen Regelungszielen des Gesetzes sind für die Privatwirtschaft vor allem zwei von Belang, da sie im Einzelfall mit erheblichen Organisations-, Investitions- und Berichtspflichten verbunden sein können: Die Stärkung der IT-Sicherheit bei sog. Betreibern Kritischer Infrastrukturen sowie die Erweiterung von Aufgaben und Kompetenzen des Bundesamts für Sicherheit in der Informationstechnik („BSI"), das nunmehr als „Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen" fungiert. Das IT-Sicherheitsgesetz ist dabei nicht als selbständiges neues Gesetzbuch konzipiert, sondern es sieht die Änderung und Ergänzung verschiedener bestehender Gesetze – insbesondere des BSI-Gesetzes[2] – vor.

Inhaltlich fügt sich das IT-Sicherheitsgesetz in die Cyber-Sicherheitsstrategie der Bundesregierung ein. Ziel dieser Anfang 2011 verabschiedeten Strategie ist es, im Zusammenwirken von Staat, Wirtschaft und Wissenschaft für Sicherheit im „Cyber-Raum" zu sorgen, ohne dessen Nutzen zu beeinträchtigen. Kernelement der Cyber-Sicherheitsstrategie ist neben der Einrichtung eines „Nationalen Cyber-Abwehrzentrums"[3] und der Gründung des „Cyber-Sicherheitsrates"[4] u.a. der nun in Form des IT-Sicherheitsgesetzes konkretisierte Schutz Kritischer Infrastrukturen.[5]

---

1 Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz); verabschiedet wurde der Gesetzentwurf der Bundesregierung vom 25. Februar 2015 (BT-Drs. 18/4096) in der vom Innenausschuss geänderten Fassung vom 10. Juni 2015 (BT-Drs. 18/5121).

2 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) vom 14. August 2009 (BGBl. I. S. 2821).

3 Informationen unter: http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Cybersicherheit/Cybersicherheitsstrategie/Cyberabwehrzentrum/cyberabwehrzentrum_node.html.

4 Informationen unter: http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Cybersicherheit/Cybersicherheitsstrategie/Cybersicherheitsrat/cybersicherheitsrat_node.html.

5 Eine Zusammenfassung der „Cyber-Sicherheitsstrategie für Deutschland" ist abrufbar unter: https://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile.

Überblick über die für Unternehmen relevanten Regelungen des IT-Sicherheitsgesetzes

1. Adressatenkreis

Hauptadressaten des IT-Sicherheitsgesetzes sind Betreiber Kritischer Infrastrukturen („BKI") in bestimmten im Gesetz abschließend aufgezählten Wirtschaftssektoren[6]. Kritische Infrastrukturen sind Einrichtungen, Anlagen oder Teile davon in einem dieser Wirtschaftssektoren, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind. Die hohe Bedeutung ergibt sich dabei daraus, dass ihr Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit zur Folge hätte. Eine konkrete Liste der betroffenen Einrichtungen und Anlagen gibt es im Gesetz nicht. Die darin abstrakt beschriebenen Kritischen Infrastrukturen werden vielmehr erst durch das Bundesinnenministerium („BMI") nach Durchführung eines komplexen Anhörungs- und Abstimmungsprozesses konkret bestimmt. Bei seiner Entscheidung über die Zugehörigkeit einer Einrichtung zur Gruppe der Kritischen Infrastrukturen hat das BMI insbesondere deren „branchenspezifischen Versorgungsgrad" zu berücksichtigen. Hierzu hat es in einem ersten Schritt branchenspezifische Schwellenwerte zu definieren, deren Über- oder Unterschreiten durch eine bestimmte Einrichtung sodann im zweiten Schritt geprüft wird. Dieses Verfahren wurde im IT-Sicherheitsgesetz festgeschrieben, um der im Gesetzgebungsverfahren wiederholt geäußerten Kritik zu begegnen, das Gesetz selbst sei in Bezug auf die Benennung der Kritischen Infrastrukturen (und damit auch in Bezug auf die Bestimmbarkeit deren Betreiber) zu vage. Wann eine bestimmte Einrichtung als einer Branche zugehörig anzusehen ist und wie der vom BMI festzustellende branchenspezifische Versorgungsgrad zu messen ist, hat der Gesetzgeber im IT-Sicherheitsgesetz nicht vorgegeben.

Es gilt derzeit als wahrscheinlich, dass neben den klassischen Unternehmen der Daseinsvorsorge wie Energie- und Wasserversorgern, Krankenhäusern, Unternehmen der Personen- und Güterbeförderung und der Lebensmittelbranche auch insbesondere größere Banken, Börsen und Finanzdienstleister Betreiber von Einrichtungen sind, die vom BMI zukünftig als Kritische Infrastrukturen definiert werden. Kleinstunternehmen, die zwar einem der im Gesetz aufgezählten Sektoren angehören, aber weniger als 10 Arbeitnehmer beschäftigen und einen Jahresumsatz von weniger als € 2 Millionen haben, sind von den Regelungen des IT-Sicherheitsgesetzes ausgenommen, auch wenn sie eine Einrichtung mit einem hohen Versorgungsgrad betreiben.

2. Pflicht zur Schaffung sicherer IT und Sorgfaltsmaßstab

Einrichtungen, die für eine Klassifizierung als Kritische Infrastruktur in Frage kommen, können einer Vielzahl verschiedener Bedrohungen ausgesetzt sein. Das IT-Sicherheitsgesetz zielt allein auf

---

Die Schaffung des IT-Sicherheitsgesetzes und die personelle Aufstockung der mit dessen Durchführung befassten Behörden war darüber hinaus Gegenstand einer Vereinbarung im Koalitionsvertrag der gegenwärtigen Bundesregierung, siehe https://www.cdu.de/sites/default/files/media/dokumente/koalitionsvertrag.pdf, S. 103.

6 Die im Gesetz enthaltene Liste von Wirtschaftssektoren umfasst die Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen. Bestimmte Branchen innerhalb dieser Sektoren sind aufgrund überlappender spezialgesetzlicher Regelungen von den Verpflichtungen des IT-Sicherheitsgesetzes befreit (siehe unten 4.).

die Bekämpfung solcher Bedrohungen ab, die von Seiten der zu ihrem Betrieb notwendigen IT-Systeme herrühren können.

Das im IT-Sicherheitsgesetz vorgesehene Pflichtenprogramm beginnt mit der Pflicht der Betreiber zur Schaffung „angemessener organisatorischer und technischer Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse“, die für die Funktionsfähigkeit ihrer Kritischen Infrastruktur erforderlich sind. Die Angemessenheit der Schutzmaßnahmen richtet sich dabei nach dem bereits aus dem Bereich der *IT-Compliance* gemäß § 91 Abs. 2 AktG bekannten Standard des „Stands der Technik“. Zur Konkretisierung des Begriffs „Stand der Technik“ verweist die Entwurfsbegründung des IT-Sicherheitsgesetzes auf nationale und internationale Normwerke sowie relevante *best practices.* Hiermit dürften insbesondere der IT-Grundschutzkatalog des BSI und die Sicherheitsstandards in der Normenreihe ISO/IEC 2007x angesprochen sein. Die zur Erreichung des Stands der Technik erforderlichen Maßnahmen sind von jedem BKI zu ergreifen, sofern sie nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur stehen.

Die Verpflichtung zur angemessen Absicherung der IT-Systeme ist dabei zwar als Soll-Vorschrift formuliert. Dies ist ausweislich der Begründung des Gesetzentwurfs aber nicht dahingehend zu verstehen, dass den BKI ein Ermessen eingeräumt würde. Vielmehr will der Gesetzgeber eine bindende Verpflichtung für alle BKI zur Wahrung des Stands der IT-Technik schaffen, von der nur in begründeten Einzelfällen abgewichen werden darf. Ein solcher Ausnahmefall soll etwa dann vorliegen, wenn eine Anpassung der IT-Systeme eines BKI an den Stand der Technik (beispielsweise durch das Aufspielen eines Software-Updates) zu einer anderweitigen Gefährdung der Einsatzfähigkeit der Kritischen Infrastruktur führen könnte, etwa aufgrund nicht abschätzbarer Inkompatibilitäten bei komplexen IT-Infrastrukturen.

Das IT-Sicherheitsgesetz zeigt sich wie auch die übrige Cyber-Sicherheitsstrategie der Bundesregierung für Beiträge aus der Wirtschaft offen: So können Unternehmen und Branchenverbände branchenspezifische Sicherheitsstandards vorschlagen, die sodann vom BSI auf ihre Eignung hin überprüft werden. Stellt das BSI fest, dass die vorgeschlagenen Sicherheitsstandards zum Schutz relevanter IT-Systeme geeignet sind, konkretisieren diese den Begriff der „angemessenen organisatorischen und technischen Vorkehrungen“, die die branchenzugehörigen BKI nach dem IT-Sicherheitsgesetz ergreifen müssen. Ziel dieser Regelung ist es, Betreibern zu ermöglichen, die Übereinstimmung von bei ihnen bereits bestehenden Schutzmechanismen mit den Anforderungen des IT-Sicherheitsgesetzes feststellen zu lassen, um ggf. unnötige Investitionen zu vermeiden.

Das vorsätzliche oder fahrlässige Außerachtlassen der Verpflichtung zur Schaffung angemessener Vorkehrungen zum Schutz seiner IT-Systeme durch einen BKI kann mit einem Bußgeld von bis zu € 50.000 durch das BSI geahndet werden. Eine zivilrechtliche Haftung von BKI gegenüber Personen, die infolge einer Verletzung dieser Verpflichtung geschädigt werden, sieht das IT-Sicherheitsgesetz selbst nicht vor. Es bleibt insoweit ggf. bei den bestehenden spezialgesetzlichen Anspruchsgrundlagen (z.B. § 7 BDSG[7]) und den allgemeinen Ansprüchen aus dem Vertrags- und Deliktsrecht (z.B. §§ 280 ff., 823 ff. BGB).[8]

---

[7] Bundesdatenschutzgesetz vom 14. Januar 2003 (BGBl. I S. 66).

[8] Anspruchsteller, die wegen einer solchen Pflichtverletzung aus § 823 BGB gegen einen BKI vorgehen möchten, dürften dabei auf die allgemeine Anspruchsgrundlage in § 823 Abs. 1 BGB beschränkt sein.

3. Dokumentations- und Berichtspflichten

Am deutlichsten über die bisher aus anderen gesetzlichen Regelungen hergeleiteten Pflichten zur Schaffung angemessener IT-Sicherheit hinaus gehen die im IT-Sicherheitsgesetz vorgesehenen Dokumentations- und Berichtspflichten. So müssen BKI die Ergreifung angemessener IT-Schutzmaßnahmen im Zweijahresrhythmus gegenüber dem BSI nachweisen und hierzu Informationen über durchgeführte Sicherheitsaudits, Prüfungen und Zertifizierungen an das BSI übersenden. Ausdrücklich aufgenommen in diese Berichtspflicht ist die Pflicht zur Mitteilung von bei derartigen Untersuchungen aufgefundenen Sicherheitsmängeln. Die Kompetenzen des BSI werden durch das IT-Sicherheitsgesetz diesbezüglich in zweierlei Hinsicht erweitert: Einerseits obliegt es dem BSI, die Anforderungen an die von den BKI durchzuführenden Sicherheitsaudits, Prüfungen und Zertifizierungen sowie die Mindestqualifikation der ausführenden Prüfstellen festzulegen. Andererseits kann das BSI die Beseitigung von Sicherheitsmängeln anordnen, die bei derlei Untersuchungen festgestellt wurden. Die Pflicht eines BKI, dieser Anordnung nachzukommen, ist mit einer Geldbuße bis zu € 100.000 bewehrt. Auch ohne eine solche Anordnung dürfte ein BKI, der einen festgestellten Sicherheitsmangel nicht von sich aus beseitigt, die im IT-Sicherheitsgesetz verankerte Verpflichtung zur Schaffung angemessener IT-Sicherheitsvorkehrungen verletzen, was für sich genommen eine bußgeldbewehrte Ordnungswidrigkeit ist (siehe oben 2.).

Für den Fall des Auftretens von Sicherheitsvorfällen ist gegenüber dem BSI von jedem BKI ein Warn- und Alarmierungskontakt zu benennen, der rund um die Uhr erreichbar sein muss. Er ist dafür zuständig, das BSI über „erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit“ der IT-Systeme von BKI zu unterrichten. Eine solche Unterrichtung muss stets erfolgen, wenn die Störung zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastrukturen führen kann oder geführt hat. Während die Mitteilung im ersten Fall („führen kann“) Angaben zur Störung und zu den technischen Rahmenbedingungen (insb. vermutete oder tatsächliche Ursache, betroffene Hard- und Software, Art der betroffenen Einrichtung oder Anlage) und zur Branche des BKI beinhalten muss, im Übrigen jedoch anonym erfolgen darf, muss die Mitteilung im zweiten Fall („geführt hat“) den BKI namentlich benennen. Zur Beseitigung einer derartigen erheblichen Störung bei einem BKI kann das BSI die Mitwirkung des Herstellers der betroffenen IT-Systeme verlangen.[9]

Das BSI ist nicht nur Sammelstelle für die Störungsmeldungen der BKI, sondern als „Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen“ auch beauftragt, Informationen zu sammeln, die die IT-Sicherheit allgemein betreffen (z.B. Informationen zu in Umlauf befindlichen Schadprogrammen oder Hacker Angriffen). Solche Informationen wertet es in Zusammenarbeit mit einer Reihe weiterer Behörden aus und analysiert dabei die potentiellen Auswirkungen auf Kritische Infrastrukturen. Gewinnt das BSI auf diese Weise Informationen, die für BKI relevant sind, hat es letztere unverzüglich zu informieren.

Weder aus dem IT-Sicherheitsgesetz noch aus der Begründung dessen Entwurfs ergibt sich nämlich eine Absicht des Gesetzgebers, mit der im IT-Sicherheitsgesetz festgeschriebenen Verpflichtung zur Schaffung angemessen geschützter IT-Systeme gerade auch einzelne Personen (im Gegensatz zur Allgemeinheit) zu schützen. Es spricht mithin viel dafür, dass die verpflichtende Norm im IT-Sicherheitsgesetz kein Schutzgesetz im Sinne des § 823 Abs. 2 BGB ist.

[9] Diese Handhabe dürfte jedoch nur gegenüber Herstellern greifen, die zumindest eine Niederlassung im Inland haben.

4. Verhältnis des IT-Sicherheitsgesetzes zu anderen Gesetzen

Gewisse Branchen sind bereits nach den auf sie anwendbaren Spezialgesetzen zur Wahrung eines bestimmten IT-Sicherheitsstandards verpflichtet. Das IT-Sicherheitsgesetz versucht Überschneidungen mit diesen Spezialgesetzen dadurch zu vermeiden, dass es sich in Bezug auf Mitglieder dieser Branchen teilweise für unanwendbar erklärt. So sind etwa Betreiber öffentlicher Telekommunikationsnetze und Erbringer öffentlich zugänglicher Telekommunikationsdienstleistungen von den Verpflichtungen des IT-Sicherheitsgesetzes befreit; sie unterfallen den entsprechenden Regelungen des TKG[10]. Entsprechendes gilt für Betreiber von Energieversorgungsnetzen sowie von Energie- und Atomanlagen, die den spezialgesetzlichen Regelungen im EnWG[11] und AtG[12] unterfallen.

Zusätzlich befreit das IT-Sicherheitsgesetz andere BKI von seinen Sicherheitsanforderungen, Berichts- und Meldepflichten, „soweit sie auf Grund von Rechtsvorschriften Anforderungen erfüllen müssen, die mit den Anforderungen“ des IT-Sicherheitsgesetzes „vergleichbar oder weitergehend“ sind. Wann ein Spezialgesetz diese Anforderungen erfüllt, ergibt sich aus dem IT-Sicherheitsgesetz selbst nicht. Die Entwurfsbegründung weist jedoch allgemein darauf hin, dass das IT-Sicherheitsgesetz nur dann gegenüber einem Spezialgesetz zurücktritt, wenn und soweit das Spezialgesetz gerade auch die IT-Sicherheit der jeweils geregelten Branche adressiert. Es ist deswegen beispielsweise naheliegend, dass Kreditinstitute aufgrund der für sie geltenden die IT-Sicherheit adressierenden Spezialregelungen in § 25a Abs. 1 KWG[13] iVm. AT. 7.2 MaRisk (2012)[14] von den Verpflichtungen des IT-Sicherheitsgesetzes ebenso befreit sind wie Versicherungen, für die § 64a Abs. 1 VAG[15] iVm. AT. 7.2.2.2 MaRisk VA (2009)[16] entsprechendes regelt. Demgegenüber ist beispielsweise eine Befreiung von Börsenträgern fraglich, da die für diese Branche geltenden Spezialgesetze die IT-Sicherheit lediglich abstrakt ansprechen, vgl. § 5 Abs. 4 BörsG[17].

Einschätzung

Die Pflicht zur Einrichtung und Überwachung eines im Hinblick auf die Datensicherheit dem Stand der Technik entsprechenden IT-Systems ergibt sich heute bereits vielfach aus *Compliance*

10 Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190).

11 Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz) vom 7. Juli 2005 (BGBl. I S. 1970, und S. 3621).

12 Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren (Atomgesetz) vom 15. Juli 1985 (BGBl. I S. 1565).

13 Gesetz über das Kreditwesen (Kreditwesengesetz) vom 9. September 1998 (BGBl. I S. 2776).

14 Rundschreiben 10/2012 (BA) der BaFin vom 14. Dezember 2012, abrufbar unter https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/rs_1210_marisk_ba.html.

15 Gesetz über die Beaufsichtigung der Versicherungsunternehmen (Versicherungsaufsichtsgesetz) vom 17. Dezember 1992 (BGBl. 1993 I S. 2).

16 Rundschreiben 3/2009 (VA) der BaFin vom 22. Januar 2009, abrufbar unter https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/rs_0903_va_marisk.html.

17 Börsengesetz vom 16. Juli 2007 (BGBl. I S. 1330).

Anforderungen und branchenspezifischen Gesetzen; sie ist grundsätzlich nichts Neues. Eine deutliche Erweiterung des bisherigen Pflichtenprogramms besteht jedoch in den vom IT-Sicherheitsgesetz vorgesehen Dokumentations- und Berichtspflichten über die vorgenommenen IT-Sicherungsmaßnahmen einerseits und Sicherheitsvorfälle andererseits. Vor allem hinsichtlich letzterer gab es während des Gesetzgebungsverfahrens eine Vielzahl kontroverser Diskussionen. So wurde insbesondere die unter bestimmten Voraussetzungen eintretende Verpflichtung zur Preisgabe nicht anonymisierter Informationen zu erheblichen Sicherheitsvorfällen und den technischen Begleitumständen gegenüber dem BSI kritisiert. Der Gesetzgeber hat diese Verpflichtung dennoch nicht nur beibehalten, sondern kurz vor Verabschiedung des Gesetzes mit einer Bußgeldbewehrung versehen. Ob diese Maßnahme die Kritik zum Verstummen bringt, darf bezweifelt werden. Dies wird vielmehr davon abhängen, ob das BSI seine Funktion als Sammelstelle von Mitteilungen der BKI einerseits und als Zentralstelle zur Bereitstellung von sicherheitsrelevanten Informationen andererseits so erfüllt, dass der vertrauliche Umgang mit den sensiblen Daten der BKI stets gewährleistet ist. Betreiber von IT-Systemen sehen nämlich in der Vertraulichkeit ihrer technischen Infrastruktur nicht nur einen strategischen Vorteil bei der Bekämpfung von IT-Angriffen. Das Bekanntwerden jeglicher Art von Sicherheitsvorfällen birgt für sie darüber hinaus ein nicht abschätzbares (Reputations-)Risiko.

Dennoch wird das Potential des IT-Sicherheitsgesetzes, zur Verbesserung der Sicherheit von IT-Systemen in Deutschland beizutragen, von Interessenverbänden und der Wissenschaft insgesamt positiv bewertet. Bis eine tatsächliche Verbesserung eintreten kann, wird aber noch einige Zeit ins Land gehen. Zunächst muss das Bundesinnenministerium nach einem umfangreichen Abstimmungsprozess die vom Gesetz nur abstrakt beschriebenen Einrichtungen konkret als Kritische Infrastrukturen benennen. Die Bundesregierung schätzt, dass etwa 2.000 Unternehmen in Deutschland als BKI einzustufen sind. Diese haben sodann zwei Jahre Zeit, ihre IT-Systeme auf den Stand der Technik zu bringen. Diese Zeit kann das BSI nutzen, um den bereits im Gesetzgebungsverfahren als zu unbestimmt kritisierten Begriff der „erheblichen Störung“ eines IT-Systems näher zu definieren und den BKI klare Leitlinien an die Hand zu geben, anhand derer sie einschätzen können, ob sie im Einzelfall einer – anonymen oder namentlichen – Meldepflicht unterliegen.

* * *

Für Fragen zu den Themen dieses Client Alert stehen Ihnen Thomas M. Buhl (tbuhl@cgsh.com), Dr. Thomas Kopp (tkopp@cgsh.com) und Matthias Schrader (mschrader@cgsh.com) aus dem Frankfurter Büro von Cleary Gottlieb sowie unsere Partner und Counsel, die auf unserer Website http://www.clearygottlieb.com/de unter Praxisbereiche – Regionen – Deutschland – Anwältinnen und Anwälte aufgeführt sind, gerne zur Verfügung.

Büros

NEW YORK
One Liberty Plaza
New York, NY 10006-1470, USA
T: +1 212 225 2000
F: +1 212 225 3999

WASHINGTON
2000 Pennsylvania Avenue, NW
Washington, DC 20006-1801, USA
T: +1 202 974 1500
F: +1 202 974 1999

PARIS
12, rue de Tilsitt
75008 Paris, Frankreich
T: +33 1 40 74 68 00
F: +33 1 40 74 68 88

BRÜSSEL
Rue de la Loi 57
1040 Brüssel, Belgien
T: +32 2 287 2000
F: +32 2 231 1661

LONDON
City Place House
55 Basinghall Street
London EC2V 5EH, England
T: +44 20 7614 2200
F: +44 20 7600 1698

MOSKAU
Cleary Gottlieb Steen & Hamilton LLC
Paveletskaya Square 2/3
Moscau, Russland 115054
T: +7 495 660 8500
F: +7 495 660 8505

FRANKFURT
Main Tower
Neue Mainzer Strasse 52
60311 Frankfurt am Main
T: +49 69 97103 0
F: +49 69 97103 199

KÖLN
Theodor-Heuss-Ring 9
50688 Köln
T: +49 221 80040 0
F: +49 221 80040 199

ROM
Piazza di Spagna 15
00187 Rom, Italien
T: +39 06 69 52 21
F: +39 06 69 20 06 65

MAILAND
Via San Paolo 7
20121 Mailand, Italien
T: +39 02 72 60 81
F: +39 02 86 98 44 40

HONGKONG
Cleary Gottlieb Steen & Hamilton (Hong Kong)
Hysan Place, 37th Floor
500 Hennessy Road
Causeway Bay
Hong Kong
T: +852 2521 4122
F: +852 2845 9026

PEKING
Cleary Gottlieb Steen & Hamilton LLP
45th Floor, Fortune Financial Center
5 Dong San Huan Zhong Lu
Chaoyang District
Beijing 100020, China
T: +86 10 5920 1000
F: +86 10 5879 3902

BUENOS AIRES
CGSH International Legal Services, LLP-
Sucursal Argentina
Avda. Quintana 529, 4to piso
1129 Ciudad Autonoma de Buenos Aires
Argentina
T: +54 11 5556 8900
F: +54 11 5556 8999

SÃO PAULO
Cleary Gottlieb Steen & Hamilton
Consultores em Direito Estrangeiro
Rua Funchal, 418, 13 Andar
São Paulo, SP Brazil 04551-060
T: +55 11 2196 7200
F: +55 11 2196 7299

ABU DHABI
Al Sila Tower, 27th Floor
Sowwah Square, PO Box 29920
Abu Dhabi, United Arab Emirates
T: +971 2 412 1700
F: +971 2 412 1899

SEOUL
Cleary Gottlieb Steen & Hamilton LLP
Foreign Legal Consultant Office
19F, Ferrum Tower
19, Eulji-ro 5-gil, Jung-gu
Seoul 100-210, Korea
T: +82 2 6353 8000
F: +82 2 6353 8099