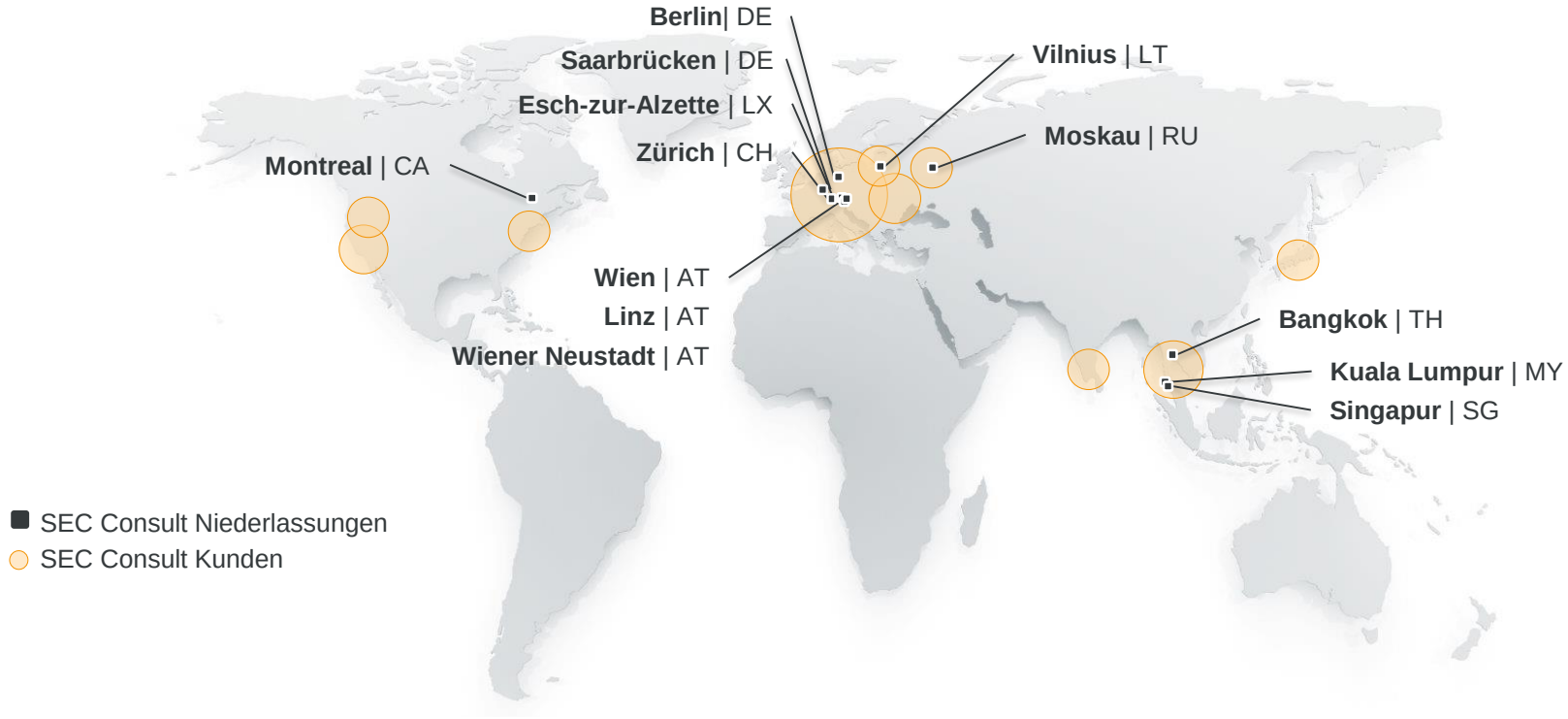
EU Datenschutz-Grundverordnung

NOCH 29 TAGE

SEC Consult
ADVISOR FOR YOUR INFORMATION SECURITY



FUNDIERTES EXPERTENWISSEN

90+ White-Hat Hacker

50+ Zertifikate

Vulnerability Lab

zahlreiche
Publikationen

LANGJÄHRIGE ERFAHRUNG

400+ Projekte / Jahr

15 Jahre Consulting

bsi. ISO/IEC 27001 Information Security Management

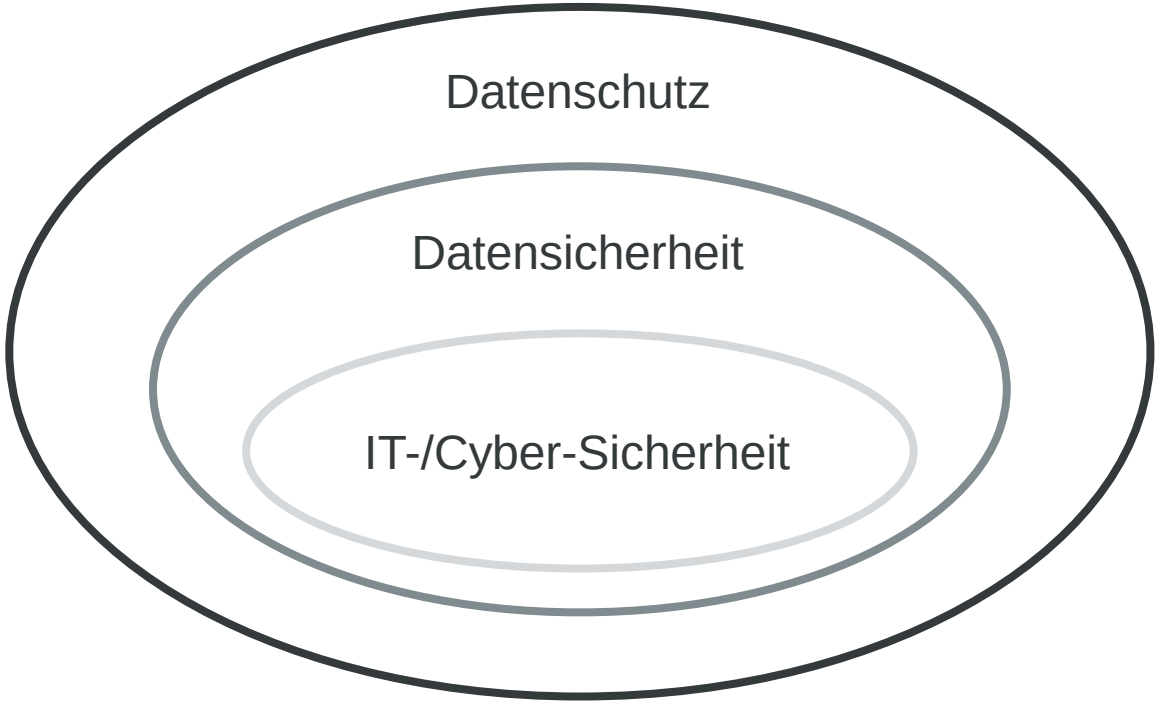
UMFANGREICHES SERVICE-PORTFOLIO

Biathlon = Zweifach-Kampf , oder?

Wie lange ist die Übergangsfrist ab dem 25.5.2018?

Bis wann sind wir fertig?

Mehr als Datenschutz…



EU-DSGVo-Scope der personenbezogenen Daten

- (Analogie zum PCI-Scope)
- Verzeichnis aller Verarbeitungstätigkeiten (mit technische Anwendungen, Services, Datenhaltungen)
- Technische Definition personenbezogener Daten
- Datenklassifizierung

DDoS Benchmark Tests

- Sicherheitstest der Anti-DDoS Maßnahmen
- Regelmäßig (lt. Gartner 1x pro Quartal)

Spezialthema „Belastbarkeit“
- Erste Schritte vs. Warten

Art 32 (1) d: „…regelmäßigen Überprüfung […] der Wirksamkeit… “

Technische Sicherheitstest

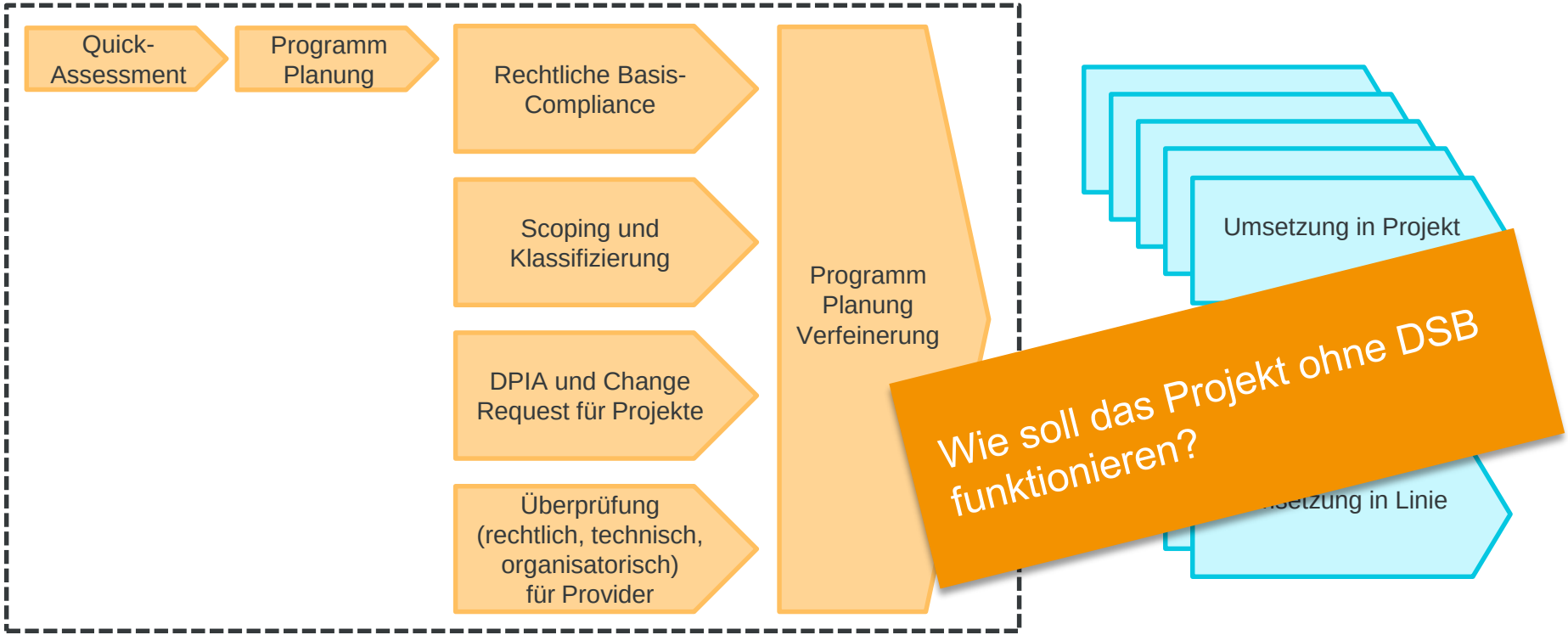
- **Penetrationstest**
- Sicherheitstest der Sicherheitsfeatures
- Regelmässig

Nachweis, Nachweis, Nachweis
- Erste Schritte vs. Warten

Organisatorische Sicherheitsaudits

- **Sicherheitsreviews** und ISMS Gap-Analysen
- Regelmässig

Art. 37: Benennung eines Datenschutzbeauftragten



Provider mit personenbezogenen Daten

- Provider-Portfolio (=Auftragsverarbeiter)
- Nachweis der Provider und aller Sub-Provider zur “hinreichend Garantien der geeignete technische und organisatorische Maßnahmen der DSGVo“ (Art 28 (3) h)
- **DSGVo-Überprüfung (rechtlich, technisch, or**

Risikoüberbindung an
Lieferanten
- Serienbriefe
- Audits

Privacy by Design

- Application Security Management (Governance)
- Sichere Software-Entwicklung (technisch/organisatorisch)
- Sichere Beschaffung von Software

Bei Software-Hersteller nur vereinzelt anzutreffen.
Implementierung bei In-house Entwicklung!

Art 32 : „Unter Berücksichtigung des Stands der Technik…“

Management der Datensicherheit

- **ISO/IEC 27001** ff.

Sprunghafter Anstieg der ISO 27001 Einführungen und Zertifizierungen

Sicherheit von Webanwendungen

- ÖNORM A 7700 (www.a7700.org)

Erhöhter Bedarf. **Achtung!** Neue Version in Q4 2018!

Art 32 (1) d: „…regelmäßigen Überprüfung […] der Wirksamkeit… “

Technische Sicherheitstest

- **Penetrationstest**
- Sicherheitstest der Sicherheitsfeatures
- Regelmäßig

Erhöhter Bedarf.
Noch kurzfristig umsetzbar!

Organisatorische Sicherheitsaudits

- **Sicherheitsreviews** und ISMS Gap-A
- Regelmäßig

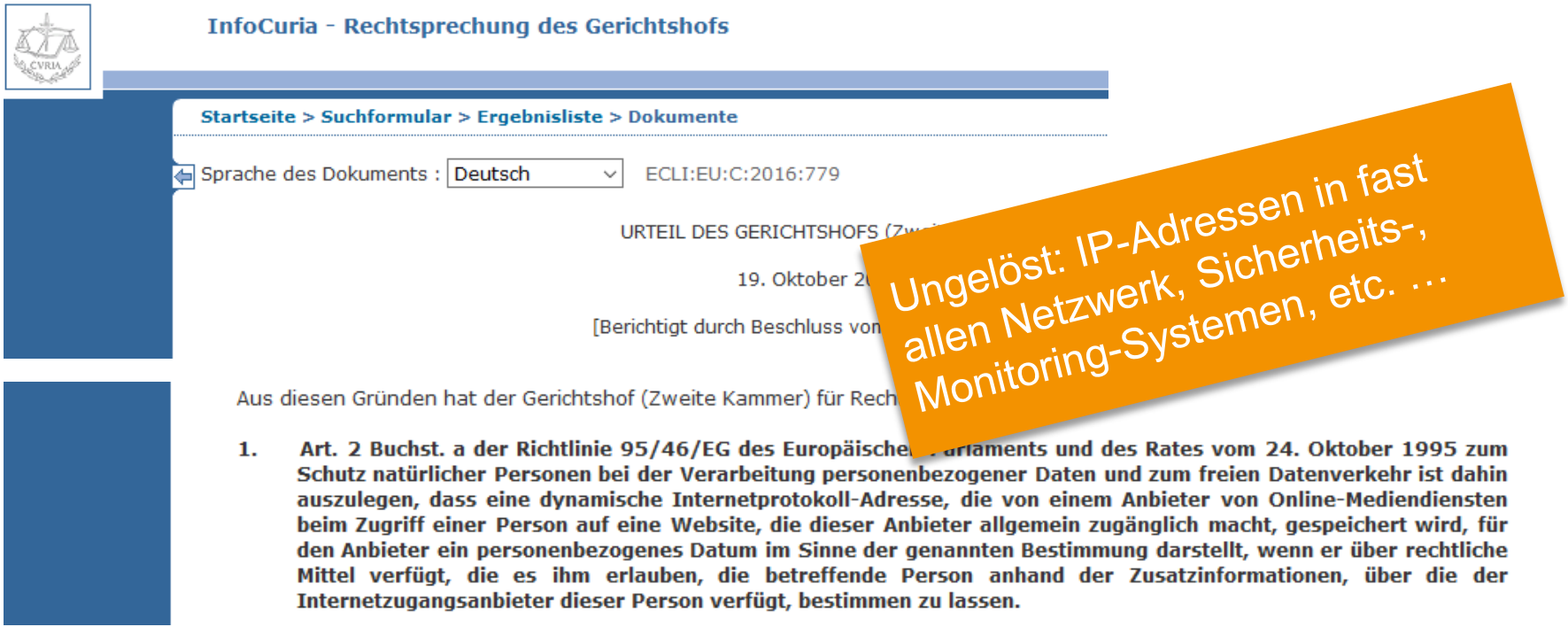
Erhöhter Bedarf.
Noch kurzfristig umsetzbar!

Incident Response und Forensik

- Hotline mit **Cyber-Security Experten 24x7**
- Onsite-Support
- DGSVO konforme Meldung

Erhöhter Bedarf.
Noch kurzfristig umsetzbar!

IP Adressen pbD (EuGH C-582/14 – Breyer)



InfoCuria - Rechtsprechung des Gerichtshofs

Startseite > Suchformular > Ergebnisliste > Dokumente

Sprache des Dokuments : Deutsch ECLI:EU:C:2016:779

URTEIL DES GERICHTSHOFS (Zw

19. Oktober 2

[Berichtigt durch Beschluss von

Aus diesen Gründen hat der Gerichtshof (Zweite Kammer) für Rech

1. **Art. 2 Buchst. a der Richtlinie 95/46/EG des Europäische[illegible]arlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ist dahin auszulegen, dass eine dynamische Internetprotokoll-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff einer Person auf eine Website, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, für den Anbieter ein personenbezogenes Datum im Sinne der genannten Bestimmung darstellt, wenn er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen.**

Ungelöst: IP-Adressen in fast allen Netzwerk, Sicherheits-, Monitoring-Systemen, etc. …

DSGVO – ein Ende in Sicht?

Prozessreifegrad		
N/A	Nicht Anwendbar	Anforderung ist auf die Organisation nicht anwendbar.
1	**Initial vorhanden / gegeben**	Die geforderten Datenschutz- & Sicherheitsmaßnahmen sind bekannt und sollen adressiert werden, jedoch sind derzeit keine Maßnahmen zur Erfüllung vorhanden.
2	**Eingeschränkt vorhanden / gegeben**	Geforderte Datenschutz-/Sicherheitsmaßnahmen sind in der Entwicklung bzw. Planung, jedoch nur mit eingeschränkt vorhandener Dokumentation. Es obliegt dem Einzelnen, diese einzuhalten.
3	**Definiert / gegeben**	Geforderte Datenschutz-/Sicherheitsmaßnahmen sind dokumentiert, kommuniziert und in die Unternehmensprozesse integriert. Mitglieder der Organisation sind verpflichtet diese einzuhalten.
4	**Gemanagt**	Die Datenschutz-/Sicherheitsmaßnahen sind vollständig dokumentiert, kommuniziert und in die Organisation integriert. Sie werden aktiv gesteuert und regelmäßig auf Angemessenheit und Wirksamkeit geprüft und zudem sind sämtliche zugrundeliegenden Risiken im Rahmen regelmäßiger Risikobewertungen identifiziert.
5	**Optimiert**	Die Datenschutz-/Sicherheitsmaßnahmen werden regelmäßig überwacht und gemessen (z.B. in QM-System integriert). Verbesserungsmaßnahmen werden anhand der Messergebnisse und Indikatoren abgeleitet, innerhalb des Verbesserungsprozesses behandelt und umgesetzt.

Focus auf welches Datum?

25.5.2018

17.8.20

Budget 2019
Planung schon begonnen?

Da war doch noch ein anderes Gesetz…

3.3 Informationsgewinnung und Datenschutz

Empfehlung 12: *Das Cybersicherheitsgesetz sollte das Themenfeld Informationsgewinnung und Datenschutz regeln. Dabei sollte das Cybersicherheitsgesetz erlauben, dass (1) Daten erfasst und ausgetauscht werden, die dazu beitragen, Cyberangriffe zu erkennen und abzuwehren, zu beseitigen und den Normalbetrieb wieder herzustellen, (2) diese Daten gespeichert werden, solange der Zweck gegeben ist und (3) Sensoren für die Datenerfassung nur auf freiwilliger Basis in private und staatliche Netze eingebaut werden können. Das Eindringen der Behörden in Computernetzwerke zur Informationsgewinnung sollte das Cybersicherheitsgesetz verbieten.*

Quelle: KSÖ Rechts- und Technologiedialog Whitepaper, Version 2.0, https://kuratorium-sicheres-oesterreich.at/wp-content/uploads/2016/06/KS%C3%96-RTD-Whitepaper.pdf

(NISG) - Netz- und Informationssystemsicherheitsgesetz
(Umsetzung EU NIS- Richtlinie)

NOCH 13 TAGE*

*Rechtzeitige nationale Umsetzung in Österreich wurde versäumt

SEC Consult in Ihrer Region (Europa)

ÖSTERREICH

SEC Consult Unternehmensberatung GmbH
Mooslackengasse 17
1190 Wien
Tel +43 1 890 30 43 0
Email office@sec-consult.com

SEC Consult Unternehmensberatung GmbH
Komarigasse 14/1
2700 Wiener Neustadt
Tel +43 2622 90568
Email office-neustadt@sec-consult.com

SEC Consult Unternehmensberatung GmbH
Wiener Straße 221
4020 Linz
Tel +43 732 917 671
Email office-linz@sec-consult.com

SCHWEIZ

SEC Consult (Schweiz) AG
Turbinenstrasse 28
8005 Zürich

Tel +41 44 271 777 0
Email office-zurich@sec-consult.com

DEUTSCHLAND

SEC Consult Deutschland Unternehmensberatung GmbH
Ullsteinstrasse 118, Turm B/8 Stock
12109 Berlin
Tel +49 30 398 20 2700
Email office-berlin@sec-consult.com

SEC Consult Deutschland Unternehmensberatung GmbH
Palais Leopold
Leopoldstraße 12
80802 München
Tel +49 30 398 20 2700
Email office-berlin@sec-consult.com

SEC Consult Deutschland Unternehmensberatung GmbH
An der Christ-König-Kirche 10
66119 Saarbrücken
Tel +49 30 398 20 2700
Email office-berlin@sec-consult.com

LUXEMBURG

SEC Consult Luxemburg S.ár.l.
25 Avenue de la gare
4131 Esch-sur-Alzette
Tel +352 265 32 330
Email office-luxembourg@sec-consult.com

LITAUEN

UAB Critical Security, a SEC Consult company
Sauletekio al. 15-311
10224 Vilnius
Tel +370 5 2195535
Email office-vilnius@sec-consult.com

RUSSLAND

Limited liability company “SEC Consult”
5th Donskoy proyezd, 15, Bldg. 11
119334, Moscow
Tel +7 495 968 77 16
Email office-moscow@sec-consult.com

SEC Consult in Ihrer Region (Asien / Nord Amerika)

MALAYSIA

SEC Consult Malaysia Sdn Bhd
Unit C-12-4, Level 12
Block C Megan Avenue II
12, Jalan Yap Kwan Seng
Kuala Lumpur

Email office-kuala-lumpur@sec-consult.com

SINGAPUR

SEC Consult Singapore PTE. LTD
4 Battery Road
#25-01 Bank of China Building
Singapur (049908)

Email office-singapore@sec-consult.com

THAILAND

SEC Consult (Thailand) Co.,Ltd.
29/1 Piyaplace Langsuan Building 16th Floor, 16B
Soi Langsuan, Ploen Chit Road
Lumpini, Patumwan | Bangkok 10330

Email office-bangkok@sec-consult.com

KANADA

i-SEC Consult Inc.
100 René-Lévesque West, Suite 2500
Montréal (Quebec) H3B 5C9

Email office-montreal@sec-consult.com

Weitere Informationen

DI Markus Robin | SEC Consult
m.robin@sec-consult.com

eudsgvo.sec-consult.com