FACHSYMPOSIUM CHINA:
DER MASTERPLAN DER VOLKSREPUBLIK - IT COMPLIANCE IN CHINA

RA RAINER BURKARDT

WIEN, 3. MAI 2018

BURKARDT & PARTNER
RECHTSANWÄLTE
上 海 申 欧 律 师 事 务 所

AGENDA
IT-COMPLIANCE

BURKARDT & PARTNER
RECHTSANWÄLTE
上 海 申 欧 律 师 事 务 所

I. Einführung

II. Daten- vs. Hardwarelokalisierung

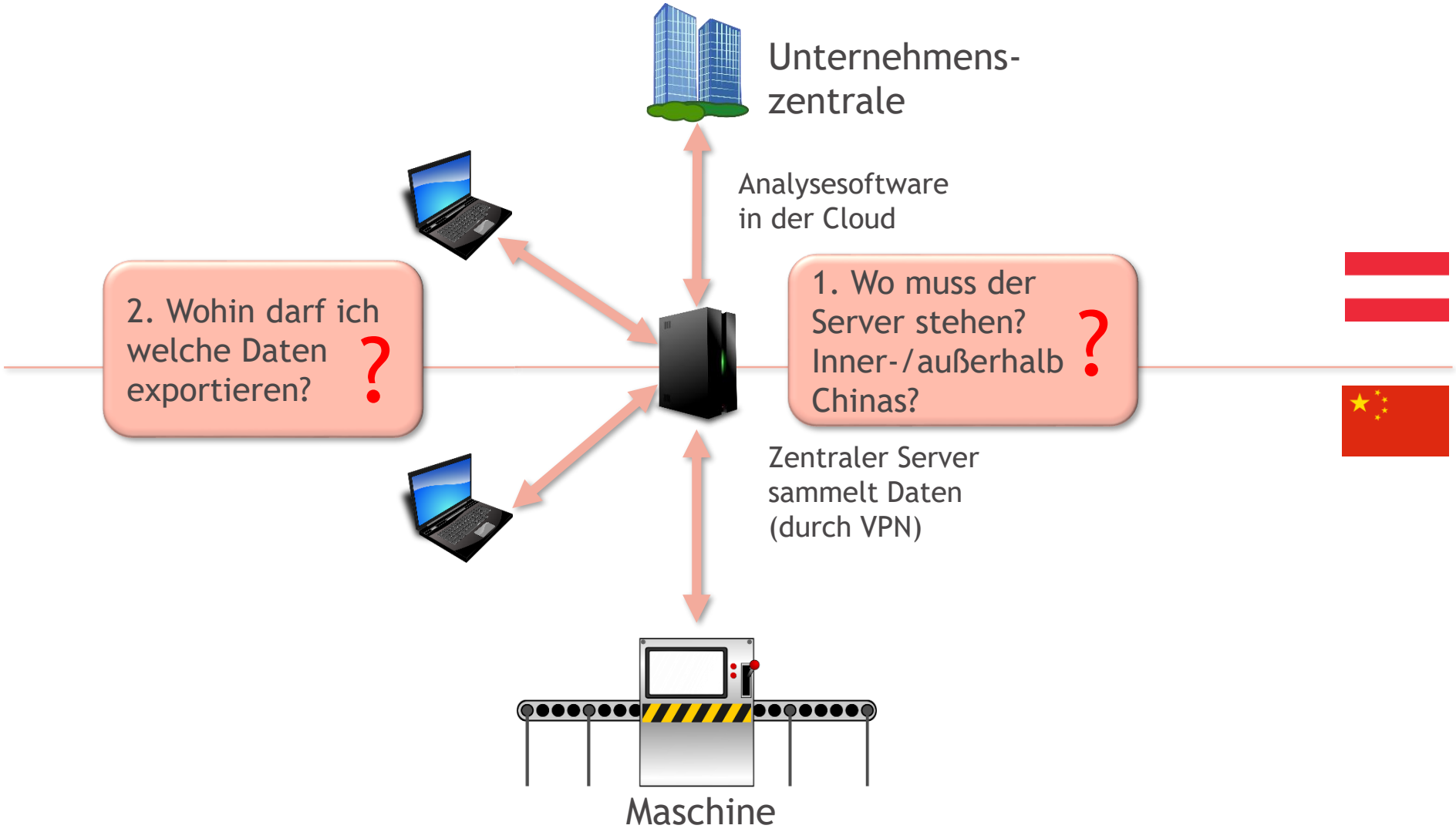
III. Kommunikationverschlüsselung

IV. Schlussfolgerung

I. EINFÜHRUNG

BEISPIEL 1: INDUSTRIE 4.0 - SPEICHERUNG UND VERARBEITUNG VON MASCHINENDATEN

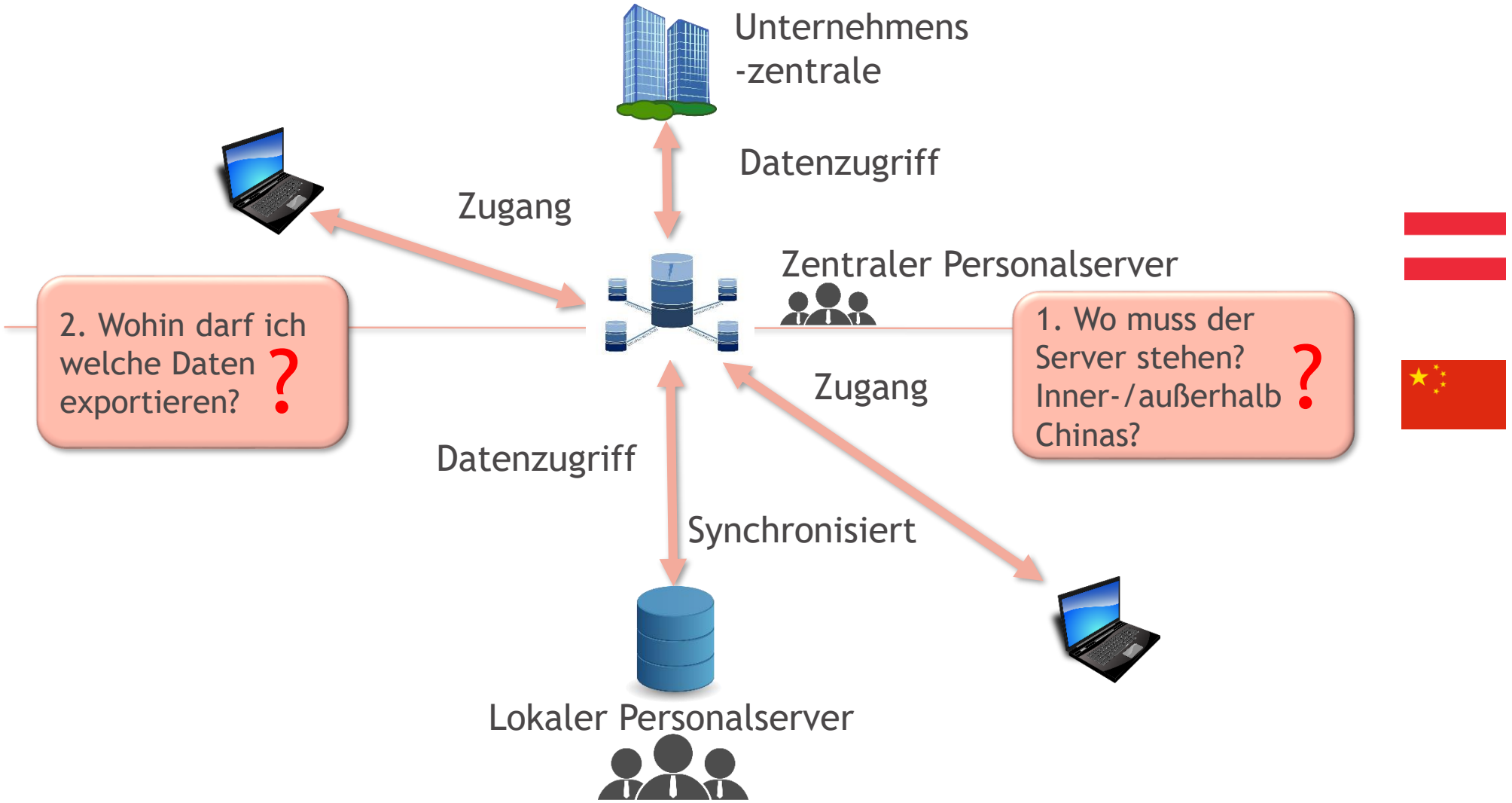
BURKARDT & PARTNER
RECHTSANWÄLTE
上 海 申 欧 律 师 事 务 所



I. EINFÜHRUNG

BEISPIEL 2: SAP - SPEICHERUNG UND VERARBEITUNG VON PERSONALDATEN

BURKARDT & PARTNER
RECHTSANWÄLTE
上 海 申 欧 律 师 事 务 所



II. DATEN- VS. HARDWARELOKALISIERUNG
DAS NETZWERKSICHERHEITSGESETZ

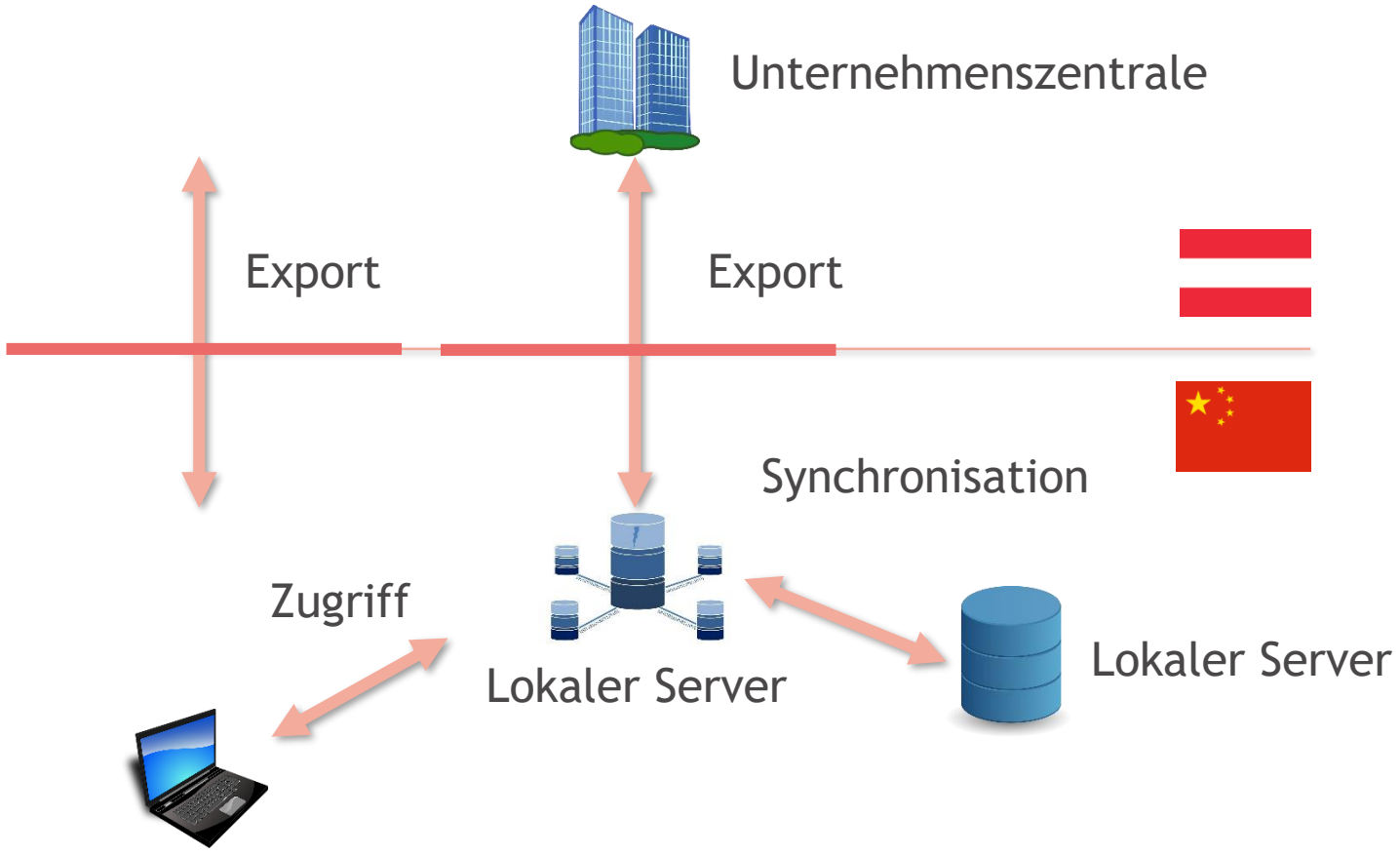
BURKARDT & PARTNER
RECHTSANWÄLTE
上 海 申 欧 律 师 事 务 所

- Speicherort von Unternehmens- und Personaldaten
  - Das Netzwerksicherheitsgesetz (“NSG” auch „Cybersecurity Law“) vom 29. Dezember 2017 bestimmt, dass ...
    - **Regel: ... persönliche Daten** und **wichtige Geschäftsinformationen** die von **kritischen Infrastrukturen** in China gesammelt werden, **in China gespeichert** werden müssen!
    - **Ausnahme:** Nur dort, wo es aufgrund von Geschäftserfordernissen notwendig ist, solche Daten und Informationen in das Ausland (Anm: Außerhalb Chinas) zu transferieren, ist ein Datenexport erlaubt, wenn eine **Sicherheitsprüfung** stattgefunden hat.
  - Ein Gesetzentwurf vom 10. Juli, 2017 erweitert diese Anforderung auf **alle Netzwerkbetreiber**
  - Definition: Ein **Netzwerkbetreiber** ist ein Nutzer, der zwei oder mehr verbundene Geräte nutzt (weitere Details noch unklar) => damit ist jeder „Netzwerkbetreiber“
  - Fehlende oder unklare Definitionen für folgende Begriffe:
    - Datenexport
    - Persönliche Daten
    - Wichtige Geschäftsinformationen
    - kritischen Infrastrukturen

II. DATEN- VS. HARDWARELOKALISIERUNG
DATENEXPORT

BURKARDT & PARTNER RECHTSANWÄLTE 上海申欧律师事务所

- Definition: **Datenexport** gilt gemäß des Informationssicherheitstechnologieentwurfs vom August 25, 2017 für...
  - ein Transfer von Daten an:
    - Unternehmen außerhalb der chinesischer Jurisdiktion
    - Unternehmen, die in China zwar registriert sind, aber keine physische Präsenz in China haben, oder
  - Daten auf die von außerhalb Chinas zugegriffen werden kann, oder
  - Daten die innerhalb einer Unternehmensgruppe an ein Gruppenmitglied außerhalb Chinas transferiert werden



II. DATEN- VS. HARDWARELOKALISIERUNG
PERSÖNLICHE DATEN

BURKARDT & PARTNER
RECHTSANWÄLTE
上 海 申 欧 律 师 事 务 所

- Definition: **Persönliche Daten** sind...
  - Verschiedene Arten von Informationen, die einzeln oder zusammen mit anderen Arten von Informationen dazu verwendet werden können eine natürliche Person zu identifizieren
  - Beispiele für Persönliche Daten sind gemäß Richtlinienentwurf:
    - Bankdaten
    - Ortsdaten
    - Eigentum
    - Telefonnummern
  - Seit 1. Mai 2018 ist eine freiwillige Datenschutzrichtline für unternehmensinterne Verarbeitung von Persönliche Daten in Kraft getreten

II. DATEN- VS. HARDWARELOKALISIERUNG
WICHTIGE GESCHÄFTSINFORMATIONEN

BURKARDT & PARTNER
RECHTSANWÄLTE
上 海 申 欧 律 师 事 务 所

- Definition: **Wichtige Geschäftsinformationen** können gemäß Richtlinienentwurf sein...
  - Daten die in Beziehung zur nationalen Sicherheit stehen, oder
  - Daten, die die wirtschaftliche Entwicklung oder gesellschaftliche und öffentliche Interessen betreffen
  - Beispiele für Wichtige Geschäftsinformationen sind Daten mit Bezug zu...
    - Gesundheit
    - Transport
    - Meterologie
    - Chemie
    - Kommunikation
  - Wobei „wichtig“ sich nicht auf das Unternemen, sondern auf staatliche Interessen bezieht.

II. DATEN- VS. HARDWARELOKALISIERUNG
KRITISCHE INFRASTRUKTUR

BURKARDT & PARTNER
RECHTSANWÄLTE
上 海 申 欧 律 师 事 务 所

- Definition: **kritischen Infrastrukturen** sind...

  - Informationssysteme oder industrielle Kontrollsysteme
  - die Netzwerkinformationsdienstleistungen für die Öffentlichkeit oder wichtige Industrien bereitstellen.
  - die, wenn ein Netzwerkssicherheitsvorkommnis eines dieser Systeme betrifft,
    - einen großen Einfluss auf den normale Betrieb wichtiger Industrien,
    - ernsthafte Schäden bei nationaler Politik, Wirtschaft, Technology, Gesellschaft, Kultur, nationaler Sicherheit, Umwelt,
    - sowie Leben und Eigentum des Volkes verursachen
  - Beispiele: Energie, Telekommunikation, Finanzen, Transport, öffentliche Ordnung

II. DATEN- VS. HARDWARELOKALISIERUNG
KRITISCHE INFRASTRUKTUR

BURKARDT & PARTNER
RECHTSANWÄLTE
上 海 申 欧 律 师 事 务 所

- Identifikationen von kritischen Industrien: Tabelle in „*Operationsleitlinie für nationale Netzwerksicherheitsprüfung*“;
- Identifikation des Informationssystems oder industriellen Kontrollsystems, welches Unternehmen oder welche Informationssysteme sich auf kritische Infrastrukturen beziehen.
- Beispiel:

Industrieprodukten (Rohmaterialien, Equipment, Verbrauchsgüter, elektronische Produktion) **1. Schritt Industriebereich**	• Betriebsmanagement • Intelligente Produktionssysteme (Industrielles Internet, IoT, Intelligente Ausrüstung) • Produktion und Verarbeitung von gefährlichen Chemikalien sowie deren Kontrolle und Lagerung (Chemie / Nuklear) • Administration und Kontrolle von Hochrisikoindustrieanlagen

2. Schritt Produktionstyp wählen

- Klassifikation (Hochrisiko) : Mehr als 5 Tote oder 50 Verletzte (bei Zwischenfall)

3. Schritt Klassifikation wählen

II. DATEN- VS. HARDWARELOKALISIERUNG
KRITISCHE INFRASTRUKTUR

BURKARDT & PARTNER
RECHTSANWÄLTE
上 海 申 欧 律 师 事 务 所

- Netzwerksicherheitsanforderungen bei kritischen Infrastrukturen:
  - Zusätzliche Sicherheitsstandards: z.B. Training von Angestellten und Führungskräften, einsetzen einer verantwortlichen Person
  - Nur Kauf von zertifiziertem Netzwerk- und Sicherheitsequipment
  - Hintergrundprüfung von verantwortlichen Personen
  - Reguläre Prüfung und Bewertung von Risiken sowie Benachrichtigung von Behörden
  - Verschwiegenheits- und Sicherheitsvereinbarungen mit Zulieferern

II. DATEN- VS. HARDWARELOKALISIERUNG
KRITISCHE INFRASTRUKTUR

BURKARDT & PARTNER
RECHTSANWÄLTE
上 海 申 欧 律 师 事 务 所

- Beispiele für Netzwerksicherheitsanforderungen:
  - Netzwerkbetreiber:
    - Einführung von Sicherheitsstandards
    - Sicherheitsspeicherung und Verschlüsselung von wichtigen Daten
    - Überwachung und Protokollierung von Netzwerkaktivitäten, sowie 6 monatigen Aufbewahrungspflicht
    - Entwurf von Notfallplänen

II. DATEN- VS. HARDWARELOKALISIERUNG
DAS NETZWERKSICHERHEITSGESETZ

BURKARDT & PARTNER RECHTSANWÄLTE 上海申欧律师事务所

- **Ausnahme:** Persönliche Daten und wichtige Geschäftsinformationen die von kritischen Infrastrukturen in China gesammelt werden, dürfen dann aus China heraus transferiert werden, wo es aufgrund von Geschäftserfordernissen notwendig ist und eine **Sicherheitsprüfung** stattgefunden hat.
- Anforderung an **Sicherheitsprüfung** (laut Entwurf):
  - Selbst durchgeführte Sicherheitsprüfung mit anschliessendem Report an die Behörden
  - Durch Behörden durchgeführte Sicherheitsprüfung
  - bei jedem Transfer oder bei dauerhafter Synchronisation einmal im Jahr
- **Ausnahme** (Sicherheitsbewertungs- und Richtlinienentwurf vom April 11 bzw. August 25, 2017): kein Datenexport ist erlaubt bei...
  - Personaldaten ohne Einverständniserklärung der betroffenen aufzuklärenden Person
  - Informationen die politische, wirtschaftliche, wissenschaftliche, militärische oder öffentliche Sicherheit bedrohen
  - Andere Daten gemäß Behördeneinzelfallentscheidungen

III . KOMMUNIKATIONSVERSCHLÜSSELUNG

VPN UND SONSTIGE VERSCHLÜSSELUNGEN

BURKARDT & PARTNER RECHTSANWÄLTE 上海申欧律师事务所

- Verschlüsselung durch und Nutzung von Virtual Private Networks ("VPN") in China
  - VPN durften noch nie verwendet werden um Internetsperren zu umgehen
  - VPN darf nur von lizensierten Drittanbietern verkauft werden
  - Interner VPN nicht offiziell verboten, bedarf aber Registrierung – Grauzone bezüglich Grenzüberschreitung
  - Seit Januar 2017 "VPN crack down"
  - Ziel des "crack down" vorrangig nicht-lizensierte Drittanbieter, weniger Private Nutzer
  - nicht-lizensierte VPN sollen gestört werden, aber technisch schwierig
- Sonstige Verschlüsselungen: Verschlüsselungsgesetz 1999
  - neuer Entwurf von 2017, aber noch nicht erlassen
  - Status:
    - Registrierung und Genehmigung ist erforderlich
    - Der Schlüssel muss an Behörden übergeben werden bei Ermittlungen (Nationale Sicherheit / Straftaten)
    - Die registrierten Verschlüsselungen können auf folgender Seite gefunden werden: State Code Administration: http://www.oscca.gov.cn/sca/index.shtml

IV. SCHLUSSFOLGERUNG

HANDLUNGSEMPFEHLUNG

BURKARDT & PARTNER
RECHTSANWÄLTE
上 海 申 欧 律 师 事 务 所

- Das NetzwerksicherheitsG ist seit 1. Mai 2018 in Kraft!
- Das NetzwerksicherheitsG ist ein Grundlagengesetz, welches zukünftig durch weitere Gesetze und Durchführungsverordnungen konkretisiert werden wird
- Zur Zeit noch viele nicht verbindliche Gesetzesentwüfe
- Sollten sich die derzeitigen Gesetzesentwürfe jedoch realisieren, dann wird dies weitreichende Auswirkungen auf viele Unternehmen und deren Daten- und IT-Infrastruktur haben
- Unternehmen sollten daher vorbeugend prüfen, ob:
  - Das Unternehmen oder dessen Kunden zur „kritischen Infrastruktur“ gehören
  - Deren Daten- und IT-Infrastruktur mit dem neuen NetzwerksicherheitsG oder schon bekannten Gesetzesentwürfen übereinstimmt
- Aufgrund von langen Vorlaufzeiten für Änderungen an der Daten- und IT-Infrastruktur empfiehlt es sich im Fall von möglichen Verstössen schon jetzt Gegenmaßnahmen zu treffen!

CONTACT

BURKARDT & PARTNER
RECHTSANWÄLTE
上 海 申 欧 律 师 事 务 所

BURKARDT & PARTNER

Room 2507, 25/F, Bund Center
222 Yanan Road East
Shanghai 200002, PR China
中国上海延安东路222号
外滩中心2507室 200002

T +86 (21) 6321 0088
F +86 (21) 6321 1100

info@BKTlegal.com
www.BKTlegal.com

Note: This presentation is for your information only and does not contain any specific statements to individual cases. Burkardt & Partner therefore assumes no liability for the content or the application on any individual case.