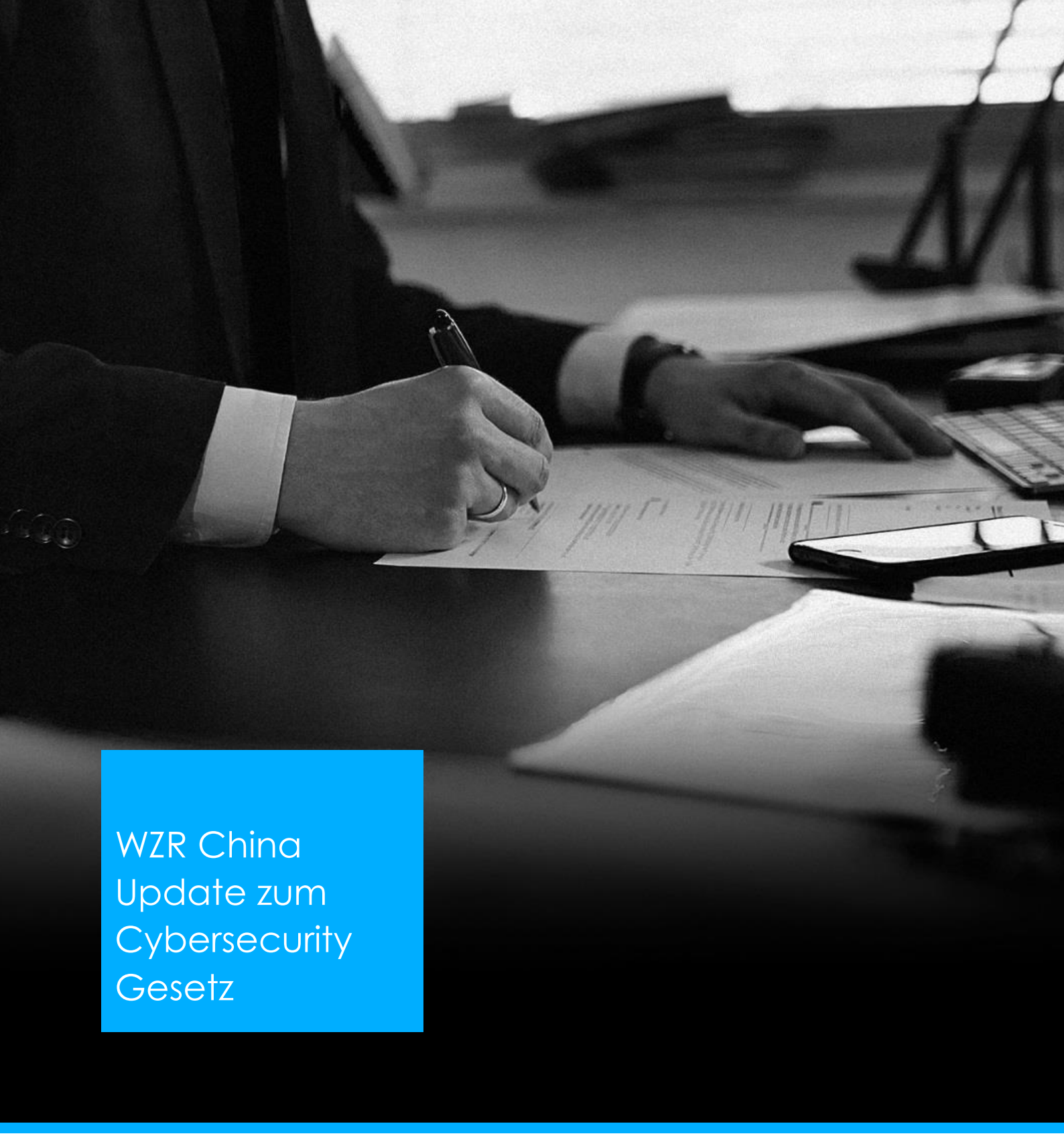


WZR China Update zum Cybersecurity Gesetz

Security Impact Assessment

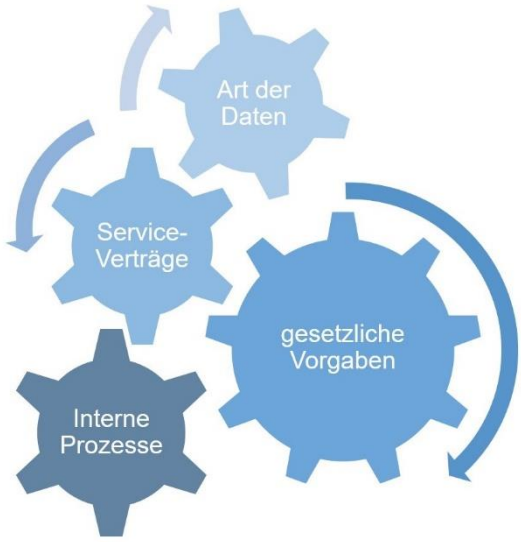
JUVE 2015 AWARDS
Kanzlei des Jahres für den Mittelstand

WZR

Security Impact Assessment – worum geht es?

Das chinesische Cybersecurity Gesetz schreibt in den Artikeln 41 ff. die Einhaltung datenschutzrechtlicher Grundsätze vor. Das Gesetz selbst sagt aber wenig dazu, wie die Anforderungen praktisch umzusetzen sind. Für die Verarbeitung personenbezogener Daten gibt der am 01.05.2018 in Kraft getretene nationale Standard „Personal Information Security Specification" (PI Security Specification) unter anderem vor, **dass Unternehmen ihre Datenverarbeitungsprozesse, hiermit verbundene Risiken und getroffene Schutzmaßnahmen in einem Security Impact Assessment dokumentieren** sollen.

Der Mitte Juni 2018 veröffentlichte Entwurf des nationalen Standards „Security Impact Assessment Guide" erklärt nun detailliert, wie Unternehmen das Assessment durchführen können.



Unternehmen sollen ihre Datenverarbeitungsprozesse aufzeichnen und dann eine Risikobewertung vornehmen. Diese ergibt sich aus dem Zusammenspiel verschiedener Faktoren, etwa

- welche Services das Unternehmen anbietet und ob diese die Verarbeitung sensitiver Daten wie z.B. Gesundheitsdaten erfordern,
- welche internen Prozesse zur Sicherung der Daten bestehen,
- ob es spezielle regulatorische Vorgaben wie Gesetze oder Standards gibt,
- ob Daten mit Dritten geteilt werden,
- welche vertraglichen Vereinbarungen mit Service-Anbietern, wie z.B. Cloud Services, getroffen werden.

Auf Grundlage dieser Aufzeichnungen und Risikobewertung können Unternehmen dann entscheiden, an welchen Stellschrauben sie drehen wollen/koennen, um in der Gesamtbewertung ein hinreichendes datenschutzrechtliches Sicherheitsniveau zu erreichen.

Security Impact Assessment – muss ich das wirklich machen?

Der Security Impact Assessment Guide ist wie die PI Security Specification ein zur Einhaltung empfohlener Standard. Unternehmen können selbst entscheiden, ob sie den Empfehlungen folgen wollen. Aufsichtsbehörden haben aber angekündigt, die PI Security Specification als Prüfungsmaßstab einzusetzen, wenn sie die Einhaltung des Cybersecurity Gesetzes prüfen. Unternehmen in China sollten den Empfehlungen deshalb nach unserer Auffassung so weit möglich folgen und nur in begründeten Ausnahmefällen abweichen.

Bei wiederholter Verletzung der datenschutzrechtlichen Regelungen des Cybersecurity Gesetzes drohen empfindliche Strafen. Artikel 64 benennt unter anderem

- Strafzahlungen bis RMB 1 Million
- Aussetzung des Geschäfts
- Sperrung Website / Online-Kanal
- Entzug der Geschäftslizenz

Security Impact Assessment – was muss ich dafür tun?

Im Rahmen des Security Impact Assessment sind verschiedene Fragestellungen abzuarbeiten. Der Umfang der erforderlichen Aktivitäten hängt dabei maßgeblich von der Größe des Unternehmens und dem Umfang der Datenverarbeitung ab. Im Rahmen der bislang vorliegenden Umsetzungsvorschriften wird kleinen und mittleren Unternehmen erstmalig zugestanden, die Maßnahmen in einem für sie „angemessenen Umfang" durchzuführen. Außerdem wird die Einschaltung externer Experten zur Durchführung des Assessments als zulässig bewertet.

Die im Security Impact Assessment Guide vorgesehenen Arbeitsschritte sind:

	Schritt	Inhalt
1	Feststellung der Erforderlichkeit eines Assessments	Grundsätzlich erforderlich, wenn ein Unternehmen personenbezogene Daten verarbeitet
2	Vorbereitungsmaßnahmen	• Benennung verantwortliche Personen • Erstellung eines Plans zur Durchführung des Assessments, Bestimmung des Umfangs der Prüfung • Einholung von Informationen bei relevanten Dritten, z.B. Service Provider
3	Aufzeichnung der Datenverarbeitungsprozesse	• Aufzeichnung aller Datenverarbeitungsprozesse von Erhebung bis Löschung personenbezogener Daten • Bezeichnung aller Beteiligen, die Zugriff auf die Daten erhalten • Bezeichnung der verwendeten Ressourcen, z.B. lokale Server, Cloud-Services
4	Prüfung der Risiken für von der Verarbeitung betroffene Personen	Feststellung der Gefahren im Falle von Datenverlusten, z.B. • Beeinträchtigung der Reputation • Diskriminierung • Vermögensschäden, z.B. durch Betrug
5	Prüfung der Wahrscheinlichkeit von Sicherheitsfällen	Feststellung der internen und externen Sicherheitsmaßnahmen, z.B. • Bestehen technischer Maßnahmen • Bestehen interner Prozesse zum Umgang mit Sicherheitsfällen • Vereinbarungen mit und Maßnahmen von Dritten, z.B. Service Provider
6	Analyse weiterer Risiken	Prüfung des allgemeinen Risikos anhand von Faktoren wie z.B. • Umfang der personenbezogenen Daten • Umfang sensitiver personenbezogener Daten
7	Erstellung eines Assessment-Reports, Feststellung von Sicherheitslücken	Siehe unten
8	Beseitigung von Sicherheitslücken	Sofern Bericht Sicherheitslücken feststellt, Anpassung der datenschutzrechtlichen Maßnahmen nach Bedarf
9	Überprüfung und Anpassung des Berichts und der Maßnahmen	• Regelmäßige Prüfung, ob Inhalte noch aktuell sind (mindestens jährlich) • Aktualisierung bei Einführung und Änderung von relevanten Services und Leistungen

Security Impact Assessment Report – was steht drin?

Mit dem Security Impact Assessment dokumentieren Sie als Unternehmen, dass Sie sich um die Einhaltung der datenschutzrechtlichen Vorschriften kümmern. Der Report ist damit ein wichtiges Mittel, um gegenüber Aufsichsbehörden Compliance nachzuweisen. Daneben ist die Erstellung des Reports für Sie ein internes Managment-Tool, mit dem bestehende Risiken identifiziert und Prozesse angepasst werden koennen.

Wesentliche Inhalte des Reports sind:

- Beschreibung der umfassten Prozesse, Arbeitsmethoden, zugrundegelegte Gesetze und Regelungen, beteiligte Personen auf Seiten des Unternehmens und Personen und Unternehmen, von denen weitere Informationen eingeholt wurden.
- Aufzeichnungen zu den Schritten 3 – 6 (siehe oben) und zur Feststellung von Sicherheitslücken

Für die Aufzeichnungen zu den Schritten 3 – 6 und die Feststellung von Sicherheitslücken gibt der Security Impact Assessment Guide ein tabellarisches Format vor. Für die *Erfassung der Datenverarbeitungsvorgänge nach den Mitteln der Verarbeitung* bzw. genutzten Systemkomponenten ist dies beispielsweise wie folgt:

Mittel der Verarbeitung / System-komponente	Werden personen-bezogene Daten erfasst?	Erfasste personen-bezogene Daten	Wie werden die personen-bezogenen Daten erfasst?	Gründe für Erfassung / Verarbeitung der personen-bezogenen Daten	Sicherheits-maßnahmen
Website-Registrierung	ja	Name, Anschrift, E-Mail	Automatisiert nach Eingabe auf Website	Notwendig zur Erfüllung eines Vertrags	Verschlüsselung der Website

Daneben werden weitere Formate / Tabellen vorgeschlagen für die *Erfassung der Datenverarbeitungsvorgänge anhand des Ablaufs der Verarbeitung* im Unternehmen und für die *Erfassung der an einem Datenverarbeitungsvorgang beteiligten Personen und Services*.

Für die Abwägung der Risiken gibt der Security Impact Assessment Guide eine Vielzahl von Regelbeispielen, mit der Risikofaktoren in verschiedene Auswirkungsgrade eingeordnet werden können, z.B.

Regelbeispiel	Auswirkungsgrad
Betroffene Person wird Opfer eines Betrugsfalls und erleidet einen wirtschaftlichen Schaden	Hoch
Betroffene Person muss zusätzliche Zeit aufwenden, fühlt sich gestört	Gering

Dem gegenüber gestellt werden Regelbeispiele zur Bestimmung der Wahrscheinlichkeit eines Sicherheitsfalls, z.B.

Regelbeispiel	Wahrscheinlichkeit
Sicherheitsmaßnahmen sind inadäquat, Datenverarbeitung entspricht nicht gesetzlichen Vorgaben	Sehr Hoch
Sicherheitsmaßnahmen sind getroffen, Datenverarbeitung entspricht Best Practice, bislang sind keine Sicherheitsvorfälle aufgetreten	Gering

Für die Bewertung des Risikos gibt der Security Impact Assessment Guide dann folgende Tabelle an die Hand:

Risikolevel		Wahrscheinlichkeit			
		Gering	Mittel	Hoch	Sehr hoch
Auswirkungs-grad	Ernsthaft	Mittel	Hoch	Ernsthaft	Ernsthaft
	Hoch	Mittel	Mittel	Hoch	Ernsthaft
	Mittel	Gering	Mittel	Mittel	Hoch
	Gering	Gering	Gering	Mittel	Mittel

+

Für europäische KMU: finale Regelung abwarten und Gestaltungsfreiheit nutzen!

Bitte beachten Sie, dass der Entwurf noch nicht final erlassen ist. Bleibt es jedoch bei den Regelungen, sollten europäische KMU von der für sie vorgesehenen Gestaltungsfreiheit Gebrauch machen. Viele der erforderlichen Informationen werden auch bei Erstellung von Verfahrensverzeichnissen und der Datenschutzfolgenabschätzung nach der DSGVO abgefragt. Sofern Sie über Prozesse und Vorlagen zur Erstellung dieser Unterlagen verfügen, können diese voraussichtlich mit geringem Umfang auf die Anforderungen in China angepasst werden. Alternativ können Sie auch bereits auf Basis Ihrer Templates mit der Erfassung ihrer Verarbeitungsvorgäne beginnen und diese nach Erlass der finalen Regelung anpassen.

+

Cybersecurity-Gesetz: Ansprechpartner

Sie haben Fragen zum Cybersecurity Gesetz im Allgemeinen? Sie benötigen Unterstützung beim Aufsetzen Ihres Projekts zum Umgang mit dem Cybersecurity Gesetz oder bei der Durchführung eines Security Impact Assessments? Unsere Ansprechpartner stehen zur Verfügung:

Jost Blöchl
Senior Associate WZR Beijing
Hauptansprechpartner Cybersecurity Gesetz

T. + 86 10 6590 7595
jost.bloechl@wzr-china.com

Dr. Florian Kessler
Managing Partner WZR Beijing
Hauptansprechpartner Cybersecurity Gesetz

T. + 86 10 6590 7595
Florian.kessler@wzr-legal.com

Dieses Update ist eine unverbindliche Information von:

WZR Ltd., Beijing
Landmark Tower II, Unit 0406
8 North Dongsanhuan Road
Beijing 100004, P.R. China
Stand: 03. Juli 2018