ANFORDERUNGEN AN CLOUD-SERVICE-PROVIDER ZERTIFIZIERUNGEN VON DATENSCHUTZ-KONFORMITÄT NACH ISO 27001 UND NEU NACH ISO 27701 UND ISO 27018

Baar, 6. Februar 2020

Von: RA Lukas Fässler; MLaw Milica Stefanovic

/Volumes/DISKs-Public/06 FACHTEXTE/Datenschutzkonformität - ISO 27001-27701-27018/Cloud-Service-Anbieter - Zertifizierung Datenschutzkonformität - Aktennotiz Finale Reinschriftverersion 2-00 - 06-02-2020.docx

Datenschutzrechtliche Aspekte in Bezug auf ISO 27018 und ISO 27701

1) Einleitung

Der Cloud-Standard ISO 27018 enthält für Anbieter von Cloud-Diensten spezifische datenschutzrechtliche Anforderungen. Er bietet Überwachungsmechanismen und Richtlinien für die Implementierung von Massnahmen zum Schutz personenbezogener Daten in der Cloud. Es werden speziell datenschutzrechtliche Anforderungen aus anderen Bereichen auf Informationssicherheitsrisiken im Bereich Cloud Computing angepasst.

Der Standard ISO 27701 ist im Juli 2019 hinzugekommen. Dieser erweitert das ISMS nach ISO 27001 um datenschutzrechtliche Aspekte.[1]

2) ISO Norm 27018

Die ISO 27018 baut inhaltlich auf den bereits gegebenen Sicherheitsstandard des ISMS nach ISO-Norm 27001 auf. Die ISO 27018 verfolgt jedoch das zusätzliche Ziel, durch entsprechende Verpflichtungen das Vertrauen bei Kunden und Behörden bezüglich der Verarbeitung personenbezogener Daten in der Cloud zu schaffen.[2]

[1] Datenschutz-Berater, Nr. 12/2019, S. 280.

[2] https://www.computerwoche.de/a/die-neue-iso-iec-27018-im-ueberblick,3069892, zuletzt besucht am: 04.02.2020.

Lukas Fässler
lic.iur.Rechtsanwalt[1,2], Informatikexperte
faessler@fsdz.ch

Carmen De la Cruz
Rechtsanwältin und Notarin[1,2]
eidg. dipl. Wirtschaftsinformatikerin

Zugerstrasse 76b
CH-6340 Baar
Tel.: +41 41 727 60 80
Fax: +41 41 727 60 85
www.fsdz.ch
sekretariat@fsdz.ch
UID: CHE-349.787.199 MWST

Partnerkanzleien:

Böhni Rechtsanwälte GmbH
Roman Böhni
MLaw Rechtsanwalt[1,2]
BSc Wirtschaftsinformatik

Zugerstrasse 76b
CH-6340 Baar
Tel.: ++41 41 541 79 60
info@boehnilaw.ch
www.boehnilaw.ch

de la cruz beranek Rechtsanwälte AG
Carmen De la Cruz
Rechtsanwältin und Notarin[1,2]
eidg. dipl. Wirtschaftsinformatikerin
delacruz@delacruzberanek.com

Nicole Beranek Zanon
Rechtsanwältin und Notarin[1,2]
beranek@delacruzberanek.com

Industriestrasse 7
CH-6300 Zug
Tel.: ++41 41 710 28 50
Fax: ++41 41 710 90 76
www.delacruzberanek.com
UID: CHE-389.928.945 MWST

Lichtsteiner Rechtsanwälte und Notare
Urs Lichtsteiner
lic. iur. Rechtsanwalt[1,2], MSc (Stanford)
lichtsteiner@lilaw.ch

Baarerstrasse 10, Postfach 7517
CH-6302 Zug
Tel.: +41 41 726 90 00
Fax: +41 41 726 90 05
www.lilaw.ch
info@lilaw.ch
UID: CHE-404.805.335 MWST

Anwaltskanzlei Dr. Weltert
Hans M. Weltert
Dr. iur. Rechtsanwalt[1,4]
hans.weltert@raweltert.ch

Matthias Heim
lic.iur. Rechtsanwalt[1,4]
matthias.heim@raweltert.ch

Michael Heim
lic.iur. Rechtsanwalt[1,4]
michael.heim@raweltert.ch

Bahnhofstrasse 10
CH-5001 Aarau
Tel.: +41 62 832 77 33
Fax: +41 62 832 77 34
www.raweltert.ch
info@raweltert.ch
UID: CHE-100.877.506 MWST

[1] Mitglied des Schweizerischen Anwaltsverbandes
[2] Eingetragen im Anwaltsregister des Kantons Zug
[3] Eingetragen im Anwaltsregister des Kantons Zürich
[4] Eingetragen im Anwaltsregister des Kantons Aargau

Die ISO 27018 enthält folgende Verpflichtungen für Cloud-Anbieter:[3]

- Personenbezogene Daten dürfen **ausschliesslich** in Übereinstimmung mit den Vorgaben der Kunden verarbeitet werden.
- Kunden müssen im Falle der Wahrnehmung von Betroffenenrechten unterstützt werden: Die ISO 27018 verlangt, dass **Cloud-Anbieter Tools offerieren**, die ihren Kunden bei der Verpflichtung helfen, Endnutzern Zugang zu persönlichen Daten zu gewähren beziehungsweise diese zu ändern, zu löschen oder korrigieren zu können.
- Die Herausgabe von Daten an Strafverfolgungsbehörden darf nur **bei vorliegender rechtlicher Verpflichtung erfolgen**. Der betroffene Kunde muss vor der Herausgabe an diese Behörden davon in Kenntnis gesetzt werden, es sei denn, diese Information ist explizit (gestützt auf spezifische gesetzliche Gründe) rechtlich untersagt.
- Die Offenlegung aller relevanten Unterbeauftragungsverhältnisse sowie der Länder, in denen eine Datenverarbeitung zusätzlich stattfindet, muss vor Vertragsschluss gegenüber dem Kunden erfolgen.
- Cloud-Anbieter müssen jede Art von **Sicherheitsverletzungen**, mit dazugehörigem Datum und den daraus zu erwartenden Konsequenzen sowie die einzelnen Schritte zur Lösung des Problems dokumentieren. Sicherheitsverletzungen müssen unverzüglich gegenüber dem Kunden angezeigt werden.
- Die Kunden müssen bei der Wahrnehmung ihrer Anzeigepflichten im Fall von Verstössen gegen die Datensicherheit vom Cloud-Serviceprovider angemessen unterstützt werden.
- Es müssen verbindliche Regeln für die **Übermittlung, Rückgabe und Verwendung** personenbezogener Daten implementiert werden, zum Beispiel im Falle der Vertragsbeendigung.
- Die Cloud-Service-Anbieter müssen sich verpflichten, die angebotenen Cloud-Dienstleistungen in regelmässigen Intervallen oder aber bei größeren Systemumstellungen **durch unabhängige Dritte überprüfen** zu lassen.

Dementsprechend können sich Cloud-Anbieter nach ISO 27018 zertifizieren lassen. Diesbezüglich müssen sie sich in regelmässigen Zeitabständen von unabhängigen Stellen erneut prüfen lassen. Der Zertifizierungsprozess bringt für einen Cloud-Nutzer erhebliche Vorteile mit sich. Da jedoch die ISO-Norm 27018 in den Bereich der ISO-Standard-Norm 27001 gehört, ist im Moment nicht geklärt, ob ISO 27018 alleine zertifiziert werden kann oder nur als Teil einer vorgängig erfolgreich durchgeführten Zertifizierung nach ISO 27001 möglich ist.

3) ISO Norm 27701

Die internationale Organisation für Normung (ISO) hat mit der ISO 27701 eine neue, zusätzliche Norm zum Nachweis der Einhaltung datenschutzrechtlicher Vorschriften veröffentlicht. Die ISO 27701 gilt als Add-On. Sie unterscheidet sich von der bereits genannten Norm ISO 27001 lediglich vorerst um eine Ziffer 7 an dritter Stelle und zeigt dadurch ihre Nähe zu ISO 27001. Die neue ISO Norm 27001 befasst sich mit den generellen Anforderungen an ein ISMS (Information Security Management System) und ermöglicht auf dieser Basis eine entsprechende Zertifizierung. Die ISO 27701 wird lediglich um die spezifischen Aspekte des Datenschutzes erweitert. Die Norm ISO 27701 soll vor allem den Bestimmungen der DSGVO u.a. hinsichtlich Dokumentationsverpflichtungen sowie Nachvollziehbarkeit entsprechen können. Datenschutz-Strukturen in Unternehmen ohne zusätzliche Einbindung eines Datenschutz-Management-System werden als unzureichend empfunden.[4] Die neue Norm ISO 27701 baut vollständig auf ISO

[3] https://www.computerwoche.de/a/die-neue-iso-iec-27018-im-ueberblick,3069892, zuletzt besucht am 04.02.2020.

[4] https://www.datenschutzbeauftragter-online.de/iso-27701-zertifizierungs-standard-privacy-management-system/13788/, zuletzt besucht am 05.02.2020.

27001 auf. Diesbezüglich müssen für eine Konformität mit der ISO 27701 alle Punkte der ISO 27001 vorab erfüllt sein. Neu ist, dass statt von «Informationssicherheit» nun die Rede ist von «Informationssicherheit und Datenschutz».[5] Vorgestellt wird diese neue ISO Norm 27701 als «Privacy Management System» aufbauend auf einer bestehenden Zertifizierung nach ISO 27001/27002. Die ersten ausländischen Unternehmen wurden bereits danach zertifiziert.[6]

Die ISO 27701 enthält zusätzliche Ergänzungen zur ISO 28002, dem Leitfaden zur Umsetzung der Massnahmen aus Anhang A der ISO 27001. Folgende Hinweise sind hierzu in der ISO 27701 enthalten:[7]

- Erweiterung der Leitlinie und der Richtlinien um Aspekte des Datenschutzes
- Ernennen eines Verantwortlichen für das „Privacy Information Management System"
- Datenschutz-Schulung der Mitarbeiter
- Protokollierung von Zugriffen und Veränderungen
- Verschlüsselung, z.B. besonderer Kategorien personenbezogener Daten (bspw. Gesundheitsdaten)
- Berücksichtigung des „Privacy by Design" Grundsatzes
- Überprüfung von Sicherheitsvorfällen auf Datenschutzverletzungen

Die ISO 27701 enthält im Anhang eine ausführliche Zuordnungstabelle der Massnahmen zu den Anforderungen der DSGVO. Diesbezüglich kann man deutlich erkennen, welchen Einfluss die DSGVO auf die ISO 27701 als internationalen Standard zum Datenschutz genommen hat.[8]

In Art. 42 DSGVO sieht die Datenschutz-Grundverordnung die Möglichkeit einer Zertifizierung explizit vor. Die Anforderungen, welche eine mögliche Zertifizierungsstelle dabei einhalten muss, beschreibt Art. 43 DSGVO. Da es sich bei der ISO 27701 um eine Erweiterung der ISO 27001 handelt, stehen auch hier Managementsysteme (ISMS) sowie Anforderungen an dieses ISMS im Mittelpunkt. Die DSGVO jedoch sieht eine Zertifizierung von Datenschutz-Management-Systemen ausdrücklich nicht vor. Doch die neue Norm endet mit einer Ziffer 1. Damit kann diese Norm zur Grundlage für Zertifzierungs-Angebote aus dem ISO-Umfeld herangezogen werden. Für einige Unternehmen ist es diesbezüglich wichtig, zur ihrer bereits bestehenden ISO 27001 noch eine ISO 27701 Zertifizierung hinzuzufügen. Der ISO 27701 Standard hilft Organisationen dabei, die eigenen Prozesse, Services und Aktivitäten mit den gesetzlichen Bestimmungen des neuen Datenschutz-Rechts (DSGVO) in Einklang zu bringen.

4) Fazit

Es ist wichtig zu wissen, dass für eine offizielle DSGVO-Zertifizierung noch Genehmigungsentscheidungen von den europäischen Regulierungsbehörden ausstehend sind.

- Es wird jedoch allen **Cloud-Service-Anbietern** empfohlen, neben der Zertifizierung nach ISO 27001 zu prüfen, ob eine Erweiterung nach den Anforderungen von ISO 20701 und ISO 27018 nicht angezeigt
- Für **Kunden von Cloud-Services** ist anzumerken, dass sie im Rahmen der ihnen vorgeschriebenen Datenschutz-Folgenabschätzung ein besonderes Augenmerk auf die Risiken legen müssen, die durch die Auslagerung von personenbezogen Daten an

[5] https://www.datenschutzbeauftragter-info.de/iso-27701-keine-zertifizierung-fuer-den-datenschutz/, zuletzt besucht am 04.02.2020.
[6] https://www.datenschutzbeauftragter-online.de/iso-27701-zertifizierungs-standard-privacy-management-system/13788/, zuletzt besucht am 05.02.2020.
[7] https://www.datenschutzbeauftragter-info.de/iso-27701-keine-zertifizierung-fuer-den-datenschutz/, zuletzt besucht am 04.02.2020.
[8] https://www.datenschutzbeauftragter-info.de/iso-27701-keine-zertifizierung-fuer-den-datenschutz/, zuletzt besucht am 04.02.2020.

Cloud-Service-Anbieter, insbesondere an solche mit Standorten und Betriebsorten im Ausland (vorab ausserhalb der Europäischen Union), entstehen. Die Unternehmen sind als Kunde in der Regel zur Kontrolle der weisungsgebundenen Cloud-Service-Anbieter verpflichtet. Wir empfehlen daher allen Kunden von Cloud-Services, in Zukunft gegenüber ihren Cloud-Service-Anbietern nicht nur die Zertifizierung nach ISO 27001 zur fordern, sondern auf das Bestehen und das Erfüllen (ob freiwillig oder eingebunden in die Basis-Zertifizierung nach ISO 27001) der neuen ISO-Normen 27018 und 27701 zu bestehen. Nehmen Sie diese Anforderungen in Zukunft in ihre Pflichtenhefte oder Offertanfragen auf und handeln Sie mit dem Cloud-Service-Anbieter aus, dass er innerhalb einer angemessenen Frist (z.B. 12-18 Monate; resp. bei seiner Rezertifizierung nach ISO 27001) den Einbezug von ISO 27701 und 27018 vornimmt.

Für weitere Fragen zu den notwendigen Datenverarbeitungsverträgen mit den organisatorischen und technischen Anforderungen an den Cloud-Service-Anbieter kontaktieren Sie uns.

Ebenso sind wir in der Lage, allfällige Anfragen von Kunden an den Cloud-Service-Anbieter durch eine Vor-Ort-Ueberprüfung der getroffenen Massnahmen als unabhängige Dritte zu überprüfen und dem Cloud-Service-Anbieter – ausserhalb einer Zertifizierung – entsprechende Bescheinigungen auszustellen (z.B. Bescheinigung über das Patchen durch notwendige Citrix-Updates, um die derzeit in der Presse, Radio und TV prominent erwähnten Sicherheitslücken zu beheben).

Sie erreichen uns dazu unter der obgenannten Firmenadresse.