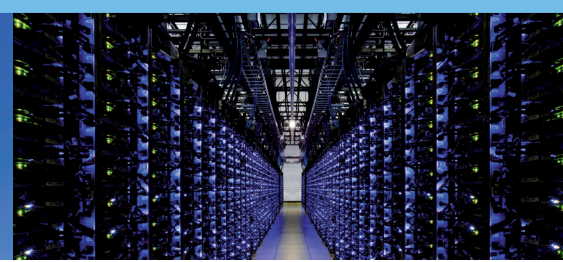


## Verhaltenskodex für den Schutz persönlicher Informationen in öffentlichen Clouds

# ISO 27018



### Worum geht es?

Bislang gab es keinen allgemeinen Standard, der sich speziell mit den datenschutzrechtlichen Anforderungen an das Cloud-Computing auseinandergesetzt hat. Dies hat sich mit der Einführung von ISO/IEC 27018 geändert. Inhaltlich baut die Norm auf bereits existierenden Sicherheitsstandards – insbesondere die ISO/IEC 27002 – auf. Allerdings befasst sich die ISO 27018 speziell mit der Regulierung der Verarbeitung von personenbezogenen Daten in einer Cloud.

### Anforderungen

- Personenbezogene Daten dürfen ausschließlich in Übereinstimmung mit den Vorgaben der Kunden verarbeitet werden.
- Die ISO 27018 verlangt, dass Cloud-Provider Tools anbieten, die ihren Kunden bei der Verpflichtung helfen, Endnutzern Zugang zu persönlichen Daten zu gewähren bzw. diese ändern, löschen und korrigieren zu können.
- Cloud-Provider haben Prozesse festzulegen, die Rückgabe, Übermittlung, Transfer und Vernichtung von personenbezogenen Daten festlegen.
- Die Herausgabe von Daten an Strafverfolgungsbehörden darf nur bei vorliegender rechtlicher Verpflichtung erfolgen.
- Personenbezogene Daten sind nicht für eigene Zwecke zu nutzen.
- Bevor personenbezogene Daten für Marketing- oder Werbezwecke genutzt werden, bedarf es einer ausdrücklichen Einwilligung des Kunden.
- Cloud-Provider haben die Länder offen zu legen, in denen eine Verarbeitung personenbezogener Daten stattfindet.
- Cloud-Anbieter müssen dem Kunden jede Art von Verletzung der Datensicherheit anzeigen und ihm diejenigen Informationen bereitstellen.
- Der Zeitraum für die Vornahme der Anzeigeverpflichtung ist festzulegen.
- Zeitpunkt, Art und Konsequenzen hinsichtlich der Verletzung der Datensicherheit sind zu dokumentieren.
- Die Anbieter müssen sich verpflichten, die angebotenen Cloud-Dienstleistungen in regelmäßigen Intervallen oder aber, bei größeren Systemumstellungen, durch unabhängige Dritte überprüfen zu lassen.

### Vorteile

In der Praxis ist der Einsatz anerkannter Sicherheitsverfahren oder aber die Zertifizierung durch unabhängige Dritte ein entscheidendes Kriterium für die Auswahl des Cloud-Anbieters. Dies gilt umso mehr für die Kontrollrechte des Auftraggebers im Rahmen einer Auftragsdatenverarbeitung nach § 11 Abs. 2 Nr. 7 BDSG.

Die ISO 27018 legt datenschutzrechtliche Anforderungen für die Anbieter von Cloud-Diensten fest und formuliert Überwachungsmechanismen und Richtlinien für die Implementierung von Maßnahmen, die den Schutz personenbezogener Daten in einer Cloud-Umgebung sicherstellen sollen. Dabei berücksichtigt die Norm datenschutzrechtliche Anforderungen, die in anderen Bereichen bereits existieren und passt diese speziell auf Informationssicherheitsrisiken im Bereich des Cloud-Computing an.

### Fazit

Die ISO 27018 ist im Gegensatz zu anderen Normen mehr als nur ein technischer Standard im Sinne von Compliance-Anforderungen, die von Unternehmen zu beachten sind.

### Umsetzung:

Durch eine 3-jährige Betreuung, Einführung, Schulung, Umsetzung und Zertifizierung dieser Managementnormen, wird der Einstieg professionell begleitet, um die gewünschte und teils geforderte Nachhaltigkeit zu erreichen.

**Eine Zertifizierung via QS-Pool ermöglicht es den einzelnen Unternehmen, die Synergieeffekte zu realisieren ohne das operative Geschäft zu stören.**



EuroConsult Deutschland GmbH  
Albertus-Magnus-Str. 2, 86836 Graben  
Telefon: +49 8232 80988-0  
Fax: +49 8232 80988-99  
info@euroconsult.de  
www.euroconsult.de

