DATENSCHUTZBEAUFTRAGTER
Schwyz - Obwalden - Nidwalden

Gotthardstrasse 21
6414 Oberarth

Datenschutz

Verwendung von Webex in der Kantonsverwaltung Schwyz

Während der Zeit der Pandemie, in der sich nur eine gewisse Zahl von Personen treffen dürfen und viele Personen zu Hause arbeiten, dürfen gewisse Lösungen zur Kommunikation vorübergehend genutzt werden. So ergibt sich basierend auf einer nicht mehr ganz aktuellen Prüfung der Datenschutzbeauftragten des Kantons Zürich aus datenschutzrechtlicher Sicht zur Verwendung von Webex als Videokonferenzlösung in der Kantonsverwaltung Schwyz Folgendes:

1. *Grundsätzlich dürfen solche Cloud-Lösungen zur Bearbeitung von Personendaten nicht genutzt werden*. Denn bei der Anwendung Webex werden Randdaten auf Servern in den USA gespeichert und nicht in den Rechenzentren in der Schweiz oder in Europa, auch wenn die Webex betreibende Firma auch in diesen Ländern/Regionen Rechenzentren haben (und dies jeweils gerne erwähnen).
   - è Begründung: Die datenschutzrechtlichen Vorgaben (wie Einräumung ausreichender Kontrollrechte für die betroffenen Personen, Gerichtsstand in der Schweiz, Datenbearbeitung / Datenlagerung / Datenspeicherung nur in der Schweiz, Schweizer Recht als anwendbares Recht etc.) können bei dieser Lösung – wie auch bei vielen anderen – nicht eingehalten werden. Erst recht gilt dies seit den Entscheiden des Europäischen Gerichtshofes betreffend Max Schrems und Facebook, die der USA kein ausreichendes Datenschutzniveau attestieren.

2. In der *momentan aufgrund der Pandemie herrschenden besonderen Lage*, in der die Ermöglichung von Arbeit per Homeoffice und ein Verbot für Treffen und somit auch für Sitzungen ab einer gewissen Anzahl (z.B. zehn) Personen besteht, können vorübergehend und auf Zusehen hin gewisse Alternativen (z.B. zur Kommunikation per Telefon- oder Videokonferenztools) notwendig werden.

3. Nun liegt es am *zuständigen* und *verantwortlichen öffentlichen Organ*, zu *entscheiden*, ob es dafür eine Cloud-Lösung nutzen und einsetzen will oder nicht. Es muss dafür aber eine *Risikoanalyse* machen und in dieser ausweisen, welche Risiken die Nutzung dieser Lösung mit sich bringt und wie es diese entsprechend minimieren will. Dazu muss es festhalten, basierend auf welcher Risiken- und Interessenabwä-gung (mit welchem Resultat) es die ausgewählte Cloud-Lösung in welchem Rahmen nutzen will (d.h. vor allem zur Bearbeitung welcher Personendaten, zu welchem Zweck und in welchem Umfang). Dabei gilt es auch die bestehenden Vorgaben der Verschlüsselung mit einzubeziehen und möglichst im Sinne der betroffenen Personen zu handeln. So sollen möglichst wenige oder nur geringe Risiken in Kauf genommen werden oder die Cloud-Lösung nur für gewisse, ganz bestimmte Zwecke verwendet werden. Das könnte z.B. bedeuten, dass diese Cloud-Lösung nur für die Kommunikation in ganz spezifischen Fällen genutzt wird, in denen man möglichst keine Personendaten bearbeiten oder zumindest und soweit möglich keine Namen nennen muss.