dsb
datenschutzbeauftragte
des kantons zürich

Checkliste für Vorabkontrolle: M365 in Gemeinde [Name der Gemeinde/Stadt einfügen]

1 Erläuterungen zur Checkliste

Die Nutzung von Microsoft 365 (M365) birgt besondere Risiken für die Grundrechte der betroffenen Personen. Deshalb untersteht sie der Vorabkontrolle durch die Datenschutzbeauftragte (DSB) (§ 10 Abs. 2 Gesetz über die Information und den Datenschutz, LS 170.4). Das Projekt M365 ist vor der Einführung der DSB vorzulegen. Sie beurteilt in der Vorabkontrolle, ob die geplante Nutzung von M365 datenschutzkonform ist.

Mit dem Leitfaden M365 in Gemeinden unterstützt die DSB die Gemeinden bei der datenschutzkonformen Einführung von M365. Die vorliegende Checkliste baut auf den Informationen des Leitfadens auf.

Die Gemeinden füllen die Checkliste aus und konsultieren dafür den Leitfaden. Die ausgefüllte Checkliste ist von der Gemeindeschreiberin oder dem Gemeindeschreiber respektive der Stadtschreiberin oder dem Stadtschreiber zu unterzeichnen. Danach ist sie für die Vorabkontrolle über das Kontaktformular an die DSB zu senden.

2 Grundinformationen

Geplanter Termin zur Migration auf M365: _____
Anzahl Nutzerinnen und Nutzer von M365: _____
Anzahl Einwohnerinnen und Einwohner: _____
Verantwortliche Person für die Einführung von M365: _____
Telefon: _____
E-Mail: _____
Beigezogenes IT-Unternehmen (falls vorhanden): _____

3 Geplantes Microsoft-Abonnement

- ☐ Office 365 E3 (Behörden)
- ☐ Office 365 E5 (Behörden)
- ☐ Microsoft 365 E3 (Behörden)
- ☐ Microsoft 365 E5 (Behörden)

Anderes:

- ☐ _____

Geplante Zusätze des Abonnements:

- ☐ Security
- ☐ Compliance
- ☐ Enterprise Mobility + Security

Andere:

- ☐ _____
- ☐ _____

4 Geplante Nutzung der Applikationen

- ☐ Advanced Threat Analytics
- ☐ Azure Active Directory
- ☐ Azure Cloud Plattform
- ☐ Bookings
- ☐ Cloud App Security
- ☐ Copilot
- ☐ Delve
- ☐ Dynamics 365
- ☐ Editor
- ☐ Exchange Online
- ☐ Forms
- ☐ Groups
- ☐ Intune
- ☐ Lists
- ☐ Loop
- ☐ Microsoft 365 Apps for Enterprise
- ☐ Microsoft Defender
- ☐ Microsoft Secure Score
- ☐ Microsoft Purview
- ☐ Microsoft Mobile Apps
- ☐ Office 365 Plattform mit Office für das Web
- ☐ OneDrive for Business
- ☐ OneNote
- ☐ Phone System
- ☐ Planner
- ☐ PowerApps
- ☐ Power Automate
- ☐ PowerBI
- ☐ Project Online
- ☐ SharePoint, SharePoint Online
- ☐ Stream
- ☐ Sway
- ☐ Syntex
- ☐ Teams
- ☐ To-Do
- ☐ Visio
- ☐ Viva Connections
- ☐ Viva Insights
- ☐ Viva Engage
- ☐ Whiteboard; Whiteboard in Teams
- ☐ Windows 365 Cloud-PC

Andere Applikationen:

- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

5 Betroffene Datenkategorien

Welche Kategorien von Daten der Gemeinde werden mit M365 bearbeitet?

- ☐ Sachdaten
- ☐ Personendaten
- ☐ Besondere Personendaten

6 Betroffene Geheimhaltungspflichten

Welchen Geheimhaltungspflichten unterliegen die Daten, die mit M365 bearbeitet werden?

- ☐ Allgemeines Amtsgeheimnis
- ☐ Besondere Amtsgeheimnisse
- ☐ Berufsgeheimnisse

7 Erforderliche Dokumente

Die folgenden Dokumente sind vollständig, aktuell und auf die Nutzung von M365 angepasst:

- ☐ Informationssicherheits- und Managementsystem (ISMS)
- ☐ Informationssicherheits- und Datenschutzkonzept für M365 (ISDS-Konzept)
- ☐ Risikoanalyse/Schutzbedarfsanalyse
- ☐ Rollen- und Berechtigungskonzept
- ☐ Nutzungsrichtlinie/-weisung für Benutzende
- ☐ Datensicherung und Notfallplanung
- ☐ Kryptokonzept (bei Verwendung eines Cloud Access Security Brokers oder dem Einsatz von Double Key Encryption)

Weitere Dokumente:

- ☐ _____
- ☐ _____
- ☐ _____

8 Zwingende Schutzmassnahmen

Wie wird verhindert, dass Microsoft einseitigen Zugriff auf besondere Personendaten und Daten unter besonderen Amtsgeheimnissen und Berufsgeheimnissen der Gemeinde hat?

- ☐ **Hybride Lösung**
  Bei der Nutzung von M365 werden besondere Personendaten und Daten unter besonderen Amtsgeheimnissen und Berufsgeheimnissen ausserhalb der Microsoft-Cloud bearbeitet und gespeichert.
  Notwendige Massnahmen:
  - ☐ Keine Verwendung von Exchange Online
  - ☐ Erstellung einer Weisung oder Richtlinie zur Nutzung der M365-Applikationen (gemäss Tabelle in Ziff. 3.1.1 Leitfaden M365 in Gemeinden)
  - ☐ Erstellung eines Schulungskonzepts zur Einhaltung der Weisung oder Richtlinie zur Nutzung der M365-Applikationen
- ☐ **Technische Lösung** mit dem Einsatz eines Cloud Access Security Broker vor Ort
  Hersteller: _____
  Produkt: _____
- ☐ **Technische Lösung** mit dem Einsatz von Double Key Encryption
- ☐ **Andere Lösung**

9 Allgemeine Schutzmassnahmen

☐ M365 ist anhand eines internationalen Standards abgesichert:
- ☐ Basis- und Standard-Anforderungen der Bausteine OPS.2.2 Cloud-Nutzung und OPS.2.3 Nutzung von Outsourcing des Deutschen Bundesamtes für Informationssicherheit (BSI)
- ☐ Empfehlungen im Handbuch «IT-Grundschutz Compliance für Office 365»
- ☐ Benchmark Level eins für M365 des Center for Internet Security (CIS)
- ☐ Auf die Umsetzung dieser Massnahmen wurde verzichtet.
  Begründung für den Verzicht:
  _____

☐ Die Konfiguration von M365 ist dokumentiert.
Datum der letzten Aktualisierung: _____
Verantwortliche Person: _____

☐ Sämtliche Konten sind mit einer Multi-Faktor-Authentifizierung (MFA) geschützt.

☐ Conditional Access wird verwendet
Wenn ja, mit folgenden Parametern:
_____

☐ Privileged Identity Management wird verwendet

☐ Als Datenspeicherorte sind ausschliesslich Länder mit angemessenem Datenschutzniveau ausgewählt.

☐ Die Übermittlung der Daten der Nutzenden (Telemetrie) ist auf ein Minimum reduziert.
Wenn ja, durch folgende Massnahmen:

10 Vertragliche Ausgestaltung

Für Gemeinden mit mindestens 250 qualifizierten Nutzenden und/oder qualifizierten Geräten:

☐ Microsoft/SIK-Rahmenvertrag 2022 wird angewendet

Für Gemeinden mit weniger als 250 qualifizierten Nutzenden und/oder qualifizierten Geräten

☐ Microsoft/SIK-Rahmenvertrag 2022 wird angewendet (Sonderregel einer einmaligen Verlängerung für bestehende Beitritte)

☐ Andere vertragliche Lösung mit Microsoft, die ein gleiches Datenschutzniveau garantiert wie der Microsoft/SIK-Rahmenvertrag, insbesondere bezüglich anwendbares Recht und Gerichtsstand) Beschreibung der vertraglichen Lösung:

11 Bestätigung

Hiermit bestätigt die [Gemeinde/Stadt] ,
dass sie M365 gemäss den Informationen in dieser Checkliste ein-führen will.

[Ort]

_____
Unterschrift
[Gemeindeschreiberin/Gemeindeschreiber – Stadtschreiberin/Stadtschreiber]
[Gemeinde/Stadt]

V 1.0 / Mai 2024