dsb
datenschutzbeauftragte
des kantons zürich

Leitfaden

Microsoft 365 in Gemeinden

Inhalt

Datenschutzbeauftragte des Kantons Zürich
Postfach, 8090 Zürich, +41 43 259 39 99
datenschutz@dsb.zh.ch, datenschutz.ch, twitter: @dsb_zh

1 Einleitung

Dieser Leitfaden richtet sich an die Gemeinden, die Microsoft 365 (M365) nutzen möchten. Er unterstützt die Projektleitung bei der datenschutzkonformen Einführung von M365.

Bei der Nutzung von M365 handelt es sich um eine Auslagerung (Bearbeiten im Auftrag im Sinne von § 6 Gesetz über die Information und den Datenschutz, IDG, LS 170.4). M365 enthält Applikationen, mit denen Informationen einer Gemeinde nicht mehr auf den eigenen Servern oder den Servern eines Hosting-Anbieters, sondern in der Cloud von Microsoft bearbeitet und gespeichert werden. Damit gehen besondere Risiken für die Grundrechte einher. Deshalb ist die beabsichtigte Nutzung von M365 der Datenschutzbeauftragten zur Vorabkontrolle einzureichen (§ 10 Abs. 2 IDG).

2 Rechtliche Rahmenbedingungen

Die Auslagerung der Datenbearbeitung an Dritte ist möglich unter Beachtung der rechtlichen Rahmenbedingungen in § 6 IDG. So dürfen der Auslagerung keine rechtlichen Bestimmungen entgegenstehen und die Gemeinde muss ihre Verantwortung für das Bearbeiten der Personendaten wahrnehmen können, auch wenn die Bearbeitung und Speicherung in einer Cloud erfolgt.

Siehe dazu Leitfaden Bearbeiten im Auftrag

2.1 Rechtsgrundlagenanalyse

Zu Beginn des Projekts ist eine Rechtsgrundlagenanalyse durchzuführen. In der Rechtsgrundlagenanalyse ist auch die Einhaltung von Geheimnispflichten (siehe Ziff. 2.3) und der Umgang mit dem US CLOUD Act zu thematisieren (siehe Ziff. 2.4).

2.2 Klassifizierung der Daten

Aus der Sicht des Datenschutzes und des Geheimnisschutzes verfügt die Gemeinde über die folgenden Arten von Daten, die von der Nutzung von M365 betroffen sein können und entsprechend zu klassifizieren sind.

Sachdaten	Informationen, die sich nicht auf bestimmte oder bestimmbare Personen beziehen Beispiele: Gesetzessammlung, Übersicht Grünanlagen
Personendaten	Informationen, die sich auf bestimmte oder bestimmbare Personen beziehen (§ 3 Abs. 3 IDG) Beispiele: Name, Vorname, Adresse, Zuteilung Schulklasse, Fahrzeugkennzeichen
Besondere Personendaten	Informationen, bei denen wegen ihrer Bedeutung, der Art ihrer Bearbeitung oder der Möglichkeit ihrer Verknüpfung mit anderen Informationen die besondere Gefahr einer Persönlichkeitsverletzung besteht (§ 3 Abs. 4 IDG) Beispiele: Strafbefehl, administrative Massnahmen, KESB-Dossier, Angaben über Sozialhilfe, Informationen über Religion, Gesundheitsdaten, Personaldossier
Besondere Amtsgeheimnisse	Informationen, die einem besonderen Amtsgeheimnis unterstehen Beispiele: Steuerdaten, Sozialhilfedaten, Opferhilfedaten
Berufsgeheimnis	Informationen, die einem Berufsgeheimnis unterstehen Beispiele: Gesundheitsdaten bei einer Ärztin oder einem Arzt

2.3 Einhaltung von Geheimnispflichten

Die von den Gemeinden bearbeiteten Personendaten können dem allgemeinen Amtsgeheimnis unterstehen (§ 8 Gemeindegesetz des Kantons Zürich, LS 131.1 und Art. 320 Strafgesetzbuch, StGB, SR 311.0). Das allgemeine Amtsgeheimnis steht einer Auslagerung nicht entgegen. Voraussetzung für eine rechtskonforme Auslagerung der Bearbeitung von Daten unter dem Amtsgeheimnis ist die vertragliche Überbindung der Geheimnispflicht an den Auftragnehmer (siehe Ziff. 2.5).

Die von den Gemeinden bearbeiteten Personendaten können auch besonderen Amtsgeheimnissen unterstehen. Beispiele für besondere Amtsgeheimnisse:

- Steuergeheimnis (§ 120 Steuergesetz des Kantons Zürich, StG, LS 631.1)
- Sozialhilfegeheimnis (§ 47 Sozialhilfegesetz des Kantons Zürich, SHG, LS 851.1)
- Opferhilfegeheimnis (Art. 11 Opferhilfegesetz, OHG, SR 312.5)

Schliesslich ist es auch möglich, dass die von den Gemeinden bearbeiteten Personendaten dem Berufsgeheimnis unterstehen (Art. 321 StGB).

Anders als das allgemeine Amtsgeheimnis stehen besondere Amtsgeheimnisse sowie das Berufsgeheimnis einer Auslagerung in die M365-Cloud entgegen, sofern die Auslagerung ein Offenbaren der Daten an Microsoft beinhaltet. Kann ein Auftragnehmer als Hilfsperson qualifiziert werden, liegt kein Offenbaren vor. Bei

Unternehmen wie Microsoft beziehungsweise deren Mitarbeitenden liegt keine Hilfspersoneneigenschaft vor. Die Nutzung von M365 kann jedoch durch technische oder organisatorische Massnahmen ermöglicht werden (siehe Ziff. 3).

2.4 Umgang mit dem US CLOUD Act

Der US CLOUD Act ist ein Gesetz der USA. Es ermöglicht bestimmten US-Behörden, amerikanische Unternehmen wie Microsoft zu verpflichten, Daten ihrer Kundinnen und Kunden herauszugeben, selbst wenn diese Daten nicht in Datenzentren in den USA gespeichert sind. Gelangt eine US-Behörde mit einer Anordnung zur Herausgabe von Personendaten an Microsoft, darf Microsoft unter Umständen die Gemeinde nicht einmal über die entsprechende Anordnung informieren, und die Gemeinde respektive die betroffenen Personen haben keine Verfahrensrechte.

Diese Zugriffsmöglichkeit ist aus datenschutzrechtlicher Sicht rechtswidrig. Deshalb dürfen Daten, die unter einem besonderen Amtsgeheimnis oder dem Berufsgeheimnis stehen, nur in der Cloud von Microsoft bearbeitet oder gespeichert werden, wenn technische Massnahmen eine einseitige Möglichkeit zur Kenntnisnahme durch Microsoft ausschliessen (siehe Ziff. 3.2). Alternativ müssen diese Daten bei der Nutzung von M365 im Rahmen einer hybriden Lösung ausserhalb der Microsoft-Cloud bearbeitet und gespeichert werden. Die Einhaltung der Trennung zwischen lokaler Bearbeitung und Cloud-Bearbeitung ist mit organisatorischen Massnahmen zu begleiten (siehe Ziff. 3.1).

Die Zugriffsmöglichkeiten unter dem US CLOUD Act führt bei der Risikoabwägung nach § 7 IDG dazu, dass Microsoft keinen Zugriff auf besondere Personendaten haben darf. Der Zugriff muss auch hier durch technische Massnahmen verhindert werden (siehe Ziff. 3.2). Alternativ müssen diese Daten im Rahmen einer hybriden Lösung ausserhalb der Microsoft-Cloud bearbeitet und gespeichert werden (siehe Ziff. 3.1).

2.5 Vertragsbeziehung mit Microsoft

Damit eine Auslagerung der Bearbeitung von Personendaten rechtmässig ist, muss ein datenschutzkonformer Vertrag mit dem Auftragnehmer abgeschlossen werden. Dieser Vertrag muss den Anforderungen von § 25 der Verordnung über die Information und den Datenschutz des Kantons Zürich (IDV, LS 170.41) genügen.

Die Schweizerische Informatikkonferenz (SIK) – neu Digitale Verwaltung Schweiz – schloss mit Microsoft einen Rahmenvertrag ab. Der SIK-Rahmenvertrag für M365 regelt unter anderem wichtige datenschutzrechtliche Punkte.

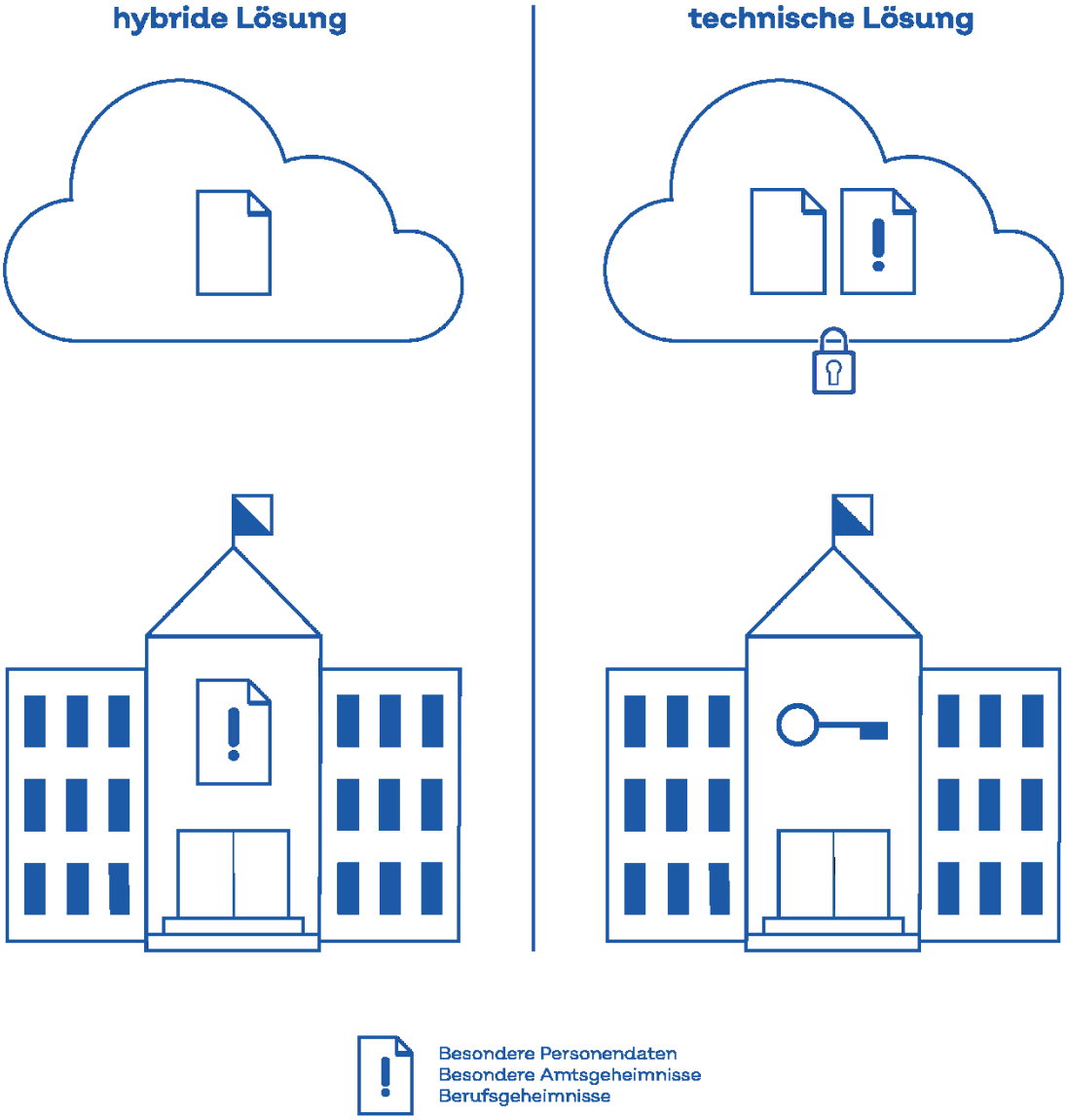
Gemeinden mit mehr als 250 qualifizierten Nutzerinnen und Nutzern oder qualifizierten Geräten können den Konzernbeitritt (EA) und den Konzern-Abonnement-Beitritt (EAS) unter dem SIK-Rahmenvertrag unterzeichnen. Die Verträge und weitere Beschreibungen können bei Digitale Verwaltung Schweiz bezogen werden.

Gemeinden mit weniger als 250 qualifizierten Nutzerinnen und Nutzern oder qualifizierten Geräten steht der SIK-Rahmenvertrag nicht zur Verfügung. Sie müssen sich an Microsoft wenden und die gleichen datenschutzrechtlichen Punkte einfordern, die mit dem SIK-Rahmenvertrag geregelt werden, inklusive Gerichtsstand Schweiz und anwendbarem schweizerischem Recht.

3 Varianten zur Umsetzung der Rahmenbedingungen

Es gibt zwei Varianten, wie M365 genutzt werden kann, so dass Microsoft keinen Zugriff auf Berufsgeheimnisse, besondere Amtsgeheimnisse und besondere Personendaten hat:

– Hybride Lösung, bei der die Daten unter dem Berufsgeheimnis und den besonderen Amtsgeheimnissen sowie die besonderen Personendaten ausserhalb der Microsoft-Cloud bearbeitet und gespeichert werden
– Technische Lösung, die eine einseitige Kenntnisnahme dieser Daten durch Microsoft ausschliesst



3.1 Hybride Lösung

Werden bei der Nutzung von M365 keine technischen Massnahmen ergriffen, die die einseitige Kenntnisnahme durch Microsoft ausschliessen (siehe Ziff. 3.2), sind besondere Personendaten sowie Daten unter besonderen Amtsgeheimnissen und Berufsgeheimnissen im Rahmen einer hybriden Lösung ausserhalb der Microsoft-Cloud zu bearbeiten und zu speichern. Sie können lokal bei der Gemeinde oder bei einem Drittanbieter ohne US-Bezug bearbeitet und gespeichert werden.

Die Applikation Exchange Online gibt es nur in der Microsoft-Cloud und kann nicht hybrid genutzt werden. Beim Erhalt von E-Mails kann nicht ausgeschlossen werden, dass besondere Personendaten und Daten unter besonderen Amtsgeheimnissen oder Berufsgeheimnissen in der Microsoft-Cloud bearbeitet und gespeichert werden. Microsoft Exchange Online kann nicht genutzt werden ohne technische Massnahmen, die die einseitige Möglichkeit zur Kenntnisnahme durch Microsoft ausschliessen (siehe Ziff. 3.2).

3.1.1 Weisung

Die Nutzung von M365 durch Mitarbeitende der Gemeinde ist in einer Weisung oder Richtlinie zu regeln. Als Hilfestellung kann die Vorlage Weisung zur Informationssicherheit in Gemeinden genutzt werden.

Zusätzlich ist in der Weisung festzuhalten, welche Arten von Daten mit welchen Microsoft-Applikationen bearbeitet werden dürfen. Beispiel hierfür ist die untenstehende Tabelle. Die Mitarbeitenden sind zur Weisung regelmässig zu schulen. Die Einhaltung der Weisung ist zu kontrollieren. Die Kontrollen sind zu dokumentieren.

Tabelle: Grundlage für die Weisung bei der hybriden Nutzung von M365

	Microsoft Applikationen							
	Office 365 Apps	Office 365 Online	Exchange Mailserver		Teams		Sharepoint	OneDrive
Klassifizierung der Daten	Word / Excel / PowerPoint lokal	Word / Excel / PowerPoint in der Cloud	Lokal oder gehostet bei Dritten[1]	Online	Audio- oder Videobesprechungen ohne Aufzeichnung	Übrige Funktionen		
Sachdaten	✓	✓	✓	✓	✓	✓	✓	✓
Personendaten	✓	✓	✓	✓	✓	✓	✓	✓
Besondere Personendaten	✓	✗	✓	✗	✓	✗	✗	✗
Besondere Amtsgeheimnisse	✓	✗	✓	✗	✓	✗	✗	✗
Berufsgeheimnisse	✓	✗	✓	✗	✓	✗	✗	✗

✓ Nutzung möglich ✗ keine Nutzung

Ausnahmen: Werden Daten **einzelfallweise** mit DKE oder CASB gegenüber Microsoft verschlüsselt, können sie auch bei der hybriden Nutzung von M365 in der Microsoft-Cloud bearbeitet und/oder gespeichert werden.

1 Unter Einhaltung der Anforderungen an die Auslagerung der Datenbearbeitung an Dritte.

3.1.2 Möglichkeiten der Verschlüsselung

Die folgenden zusätzlichen Verschlüsselungstechniken verhindern die Kenntnisnahme durch Microsoft:

- Je nach Schutzbedarf können Daten durch Double Key Encryption (DKE) oder mit speziellen Programmen wie 7zip lokal auf den Computern verschlüsselt werden, bevor sie in die Cloud gelangen.
- In der Applikation Teams kann eine Ende-zu-Ende-Verschlüsselung eingeschaltet werden. Audio- und Videodaten werden beim Sendenden verschlüsselt und beim Empfangenden entschlüsselt. Einige Funktionen wie das Aufzeichnen von Anrufen sind bei einer Ende-zu-Ende-Verschlüsselung nicht möglich.

3.2 Technische Lösung (Verschlüsselung)

Es gibt zwei technische Massnahmen, die eine einseitige Kenntnisnahme der Daten durch Microsoft verhindern. Die umfassende Nutzung der Double Key Encryption (DKE) und die umfassende Nutzung eines Cloud Access Security Broker (CASB) mit Verschlüsselung gegenüber Microsoft.

- Bei der DKE von Microsoft werden Dokumente auf dem Gerät verschlüsselt, bevor sie in die Microsoft-Cloud geladen werden. Die Verschlüsselung erfolgt mit zwei Schlüsseln. Ein Schlüssel liegt bei Microsoft, der andere bei der Gemeinde. Die Gemeinde behält die vollständige Kontrolle über ihren Schlüssel (zum Schlüsselmanagement siehe Ziff. 3.2.2).
- CASB-Lösungen verschlüsseln den Datenfluss zwischen den Geräten der Gemeinde und der Microsoft-Cloud. Die Daten werden verschlüsselt, bevor sie in der Microsoft-Cloud gespeichert werden. Microsoft hat damit keine Möglichkeit, einseitig auf Daten zuzugreifen.

Abgrenzung:
Verschlüsselungslösungen wie Bring Your Own Key (BYOK) schliessen eine einseitige Kenntnisnahme durch Microsoft nicht aus. Bei BYOK wird der Schlüssel in der Microsoft-Cloud gespeichert. Microsoft kann sich also Zugriff auf den Schlüssel verschaffen und damit auf die verschlüsselten Daten.

3.2.1 Weisung

Die Nutzung von M365 durch Mitarbeitende der Gemeinde ist in einer Weisung oder Richtlinie zu regeln. Als Hilfestellung kann die Vorlage Weisung zur Informationssicherheit in Gemeinden genutzt werden.

Je nach Produkt und Funktionsweise verschlüsselt bei CASB nur einen Teil der Daten. So wird beispielsweise die Betreffzeile meist nicht verschlüsselt. Diese Spezialfälle sind in der Weisung festzuhalten und das entsprechende Vorgehen ist zu definieren.

Die Mitarbeitenden sind regelmässig zur Weisung zu schulen. Die Einhaltung der Weisung ist zu kontrollieren. Die Kontrollen sind zu dokumentieren.

3.2.2 Schlüsselmanagement

Es ist ein Kryptokonzept zu erstellen. Darin ist unter anderem festzuhalten:

- Welche Verschlüsselungsverfahren warum verwendet werden
- Wie die Schlüssel gesichert werden (Backup)
- Wie Schlüssel erzeugt, gespeichert, ausgetauscht und wieder gelöscht werden
- Wie die Integrität und Authentizität der Schlüssel sichergestellt werden
- Wer Zugriff auf die Schlüssel hat. Dies kann auch im Rahmen des Rollen- und Berechtigungskonzepts abgehandelt werden (siehe Ziff. 4)

Weitere Informationen:

- BSI-Baustein CON.1 «Kryptokonzept»
- NIST-Guideline for Key-Management

3.2.3 Zusätzliche Massnahmen bei der Verwendung eines CASB

Eine CASB-Lösung kann lokal bei der Gemeinde oder bei einem Dritten installiert werden. Ist die Lösung lokal installiert, hat nur die Gemeinde Zugriff auf die Schlüssel und die Daten (siehe Ziff. 3.2.2). Ist die CASB-Lösung bei einem Dritten installiert, so kann er Zugriff auf die Schlüssel und damit auf die Daten haben. Entsprechend sind die Anforderungen an die Auslagerung der Datenbearbeitung an den Dritten zu beachten.

Weitere Informationen:
- Leitfaden Bearbeiten im Auftrag
- Leitfaden Verschlüsselung der Daten im Rahmen der Auslagerung
- Leitfaden Auslagerung: CLOUD Act

4 Allgemeine Massnahmen bei der Nutzung von M365

Nach der Klärung der beschriebenen rechtlichen Rahmenbedingungen ist eine Risikoanalyse durchzuführen. Dazu dient ein Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept). Die Gemeinde hat die spezifischen Risiken durch angemessene Massnahmen auszuschliessen oder auf ein tragbares Mass zu reduzieren (§ 7 IDG). Als Muster können die Vorlagen des Competence Center Projektmanagement des Kantons Zürich verwendet werden.

Das ISDS-Konzept muss unter anderem folgende Punkte umfassen:
- **Einstufung des Schutzobjekts:** Es ist eine Schutzbedarfsanalyse vorzunehmen (siehe Vorlagen).
- **Risikoanalyse und Schutzmassnahmen:** Darin sind die relevanten Risikofaktoren (Verfügbarkeit, Vertraulichkeit, Integrität und Nachvollziehbarkeit) aufzulisten, zu beschreiben, zu bewerten und mit entsprechenden Schutzmassnahmen zu minimieren (siehe Vorlagen).
- **Rollen- und Berechtigungskonzept:** Darin ist unter anderem festzulegen, welche Personengruppen (Behördenmitglieder, Personalabteilungen, Fachbereiche usw.) auf welche Applikationen und welche Daten zugreifen dürfen.
  Weitere Informationen: BSI-Baustein ORP 4 «Identitäts- und Berechtigungsmanagement» oder DSB-Vorlagen
- **Datensicherung und Notfallplanung:** Die Massnahmen zur Datensicherung und Notfallplanung sollten unter anderem einen zweiten, redundanten Internetanschluss, lokale Backups oder die Verwendung der Desktop-Version der Office-Programme beinhalten (siehe Vorlagen).

Die Nutzung von M365 setzt ein etabliertes und umfassendes Informationssicherheits- und Managementsystem (ISMS) der Gemeinde voraus. Die Datenschutzbeauftragte stellt dafür Vorlagen zur Verfügung. Es sind insbesondere die Verantwortlichkeiten und die Schutzziele zu definieren sowie eine Risikoanalyse mit den entsprechenden Massnahmen durchzuführen. Das ISDS-Konzept für M365 ist in das übergeordnete ISMS zu integrieren und die Konformität zu den entsprechenden Vorgaben ist zu prüfen.

In diesem Leitfaden werden nur M365-spezifische Schutzmassnahmen erwähnt. Die sonstigen Schutzmassnahmen für IKT-Systeme sind jedoch weiterhin umzusetzen. Dazu zählen die umfassende Nutzung eines Virenschutzes oder die regelmässige Schulung und Sensibilisierung der Mitarbeitenden.

4.1 Orientierung an internationalen Standards

Die Schutzmassnahmen für M365 orientieren sich an internationalen Standards. Dies sind beispielsweise:
- Bausteine OPS.2.2 Cloud-Nutzung und OPS.2.3 Nutzung von Outsourcing des Deutschen Bundesamtes für Informationssicherheit (BSI)
- Handbuch IT-Grundschutz Compliance für Office 365
- Sicherer Betrieb von M365 gemäss dem Center for Internet Security (CIS)

4.2 Konfigurationsmanagement

Die Konfiguration von M365 ist zu dokumentieren und regelmässig zu überprüfen. Microsoft führt laufend Updates durch, ändert Funktionen oder fügt neue hinzu. Diese Änderungen sind in der Microsoft-Roadmap ersichtlich. Hinweise auf mögliche Fehlkonfigurationen beziehungsweise Verbesserungen geben der sogenannte Secure Score von Microsoft, der CIS-Benchmark sowie interne und externe Audits.

4.3 Authentifizierung und Passwörter

Generell ist eine Multi-Faktor-Authentifizierung zu implementieren. Diese kann in M365 aktiviert werden – siehe Anleitung von Microsoft. Es können auch das TAN-Verfahren oder Einmalpasswörter eingesetzt werden. Müssen externe IT-Techniker regelmässig auf den Tenant der Gemeinde zugreifen, ist der Einsatz des Privileged Identity Management zu prüfen.

Bei hohem Risiko ist die Aktivierung des bedingten Zugriffs mit Azure AD (Conditional Access) zu prüfen. Dabei können Zugriffe mit verschiedenen Parametern geregelt werden. So kann beispielsweise der Zugriff im Büro mit Nutzernamen, Kennwort und auf dem Computer gespeicherten Zertifikat erfolgen. Im Homeoffice wird zusätzlich ein dritter Faktor verlangt.

Weitere Informationen:
- Synchronisation von Identitäten und Authentifizierung bei M365
- Integration des lokalen Active Directory in Azure Active Directory
- Bedingter Zugriff mit Azure AD

4.4 Telemetriedaten

Die lokalen M365-Programme übermitteln Telemetriedaten an Microsoft. Diese Daten enthalten Personendaten in der Form von Informationen über die Mitarbeitenden und ihre Nutzung der M365-Applikationen. Es sind insbesondere folgende Vorkehrungen zu treffen:
- Bei den Diagnosedaten ist die Option «Weder noch» zu aktivieren.
- Die «optional verbundenen Erfahrungen» sind zu konfigurieren und zentral zu deaktivieren.
- Die Teilnahme am Programm zur Verbesserung der Benutzerfreundlichkeit ist zu deaktivieren (Microsoft Customer Experience Improvement Program, CEIP).

Weitere Informationen:
- Benchmark des Center for Internet Security (CIS) für Office-Programme

4.5 Länderauswahl

Bei der Nutzung von M365 sind die Länder zu bestimmen, in denen die bearbeiteten Daten gespeichert werden. Die Daten müssen in der Schweiz oder in der EU gespeichert werden (EU-Datengrenze für die Microsoft Cloud oder auch EU Data Boundary).

5 Vorabkontrolle

5.1 Pflicht zur Vorabkontrolle

Die Nutzung von M365 in einer Gemeinde birgt besondere Risiken für die Grundrechte der betroffenen Personen. Deshalb untersteht sie der Vorabkontrolle durch die Datenschutzbeauftragte (§ 10 Abs. 2 IDG). Das Projekt ist vor der Einführung der DSB vorzulegen. Die DSB beurteilt in der Vorabkontrolle, ob die geplante Nutzung von M365 datenschutzkonform ist.

Für die Vorabkontrolle der M365-Einführung in Gemeinden sieht die Datenschutzbeauftragte ein spezifisches Vorgehen mit einer Checkliste vor.

5.2 Checkliste

Für die Vorabkontrolle füllen die Gemeinden eine Checkliste aus, die zum Leitfaden M365 für Gemeinden gehört. Diese Checkliste ist von der Gemeindeschreiberin oder dem Gemeindeschreiber respektive der Stadtschreiberin oder dem Stadtschreiber zu unterzeichnen.

Die Checkliste ist auf der Website der DSB zugänglich.

Die ausgefüllte Checkliste ist über das Kontaktformular an die DSB zu senden.

5.3 Prüfung durch die Datenschutzbeauftragte

Die DSB prüft die Checkliste und hält ihr Ergebnis in einer Stellungnahme fest. Im Rahmen ihrer Prüfung kann die DSB weitere Dokumente einfordern, beispielsweise das ISDS-Konzept oder die Datenschutz-Folgenabschätzung nach § 10 Abs. 1 IDG. Die DSB behält sich vor, die Vorabkontrolle weiter auszudehnen, beispielsweise bei grossen Gemeinden oder besonders vielen Nutzerinnen und Nutzern.

V 1.0 / Juni 2024