LfDI Baden-Württemberg **22. April 2021**

Pilotprojekt Nutzung Microsoft 365 an Schulen:

Umsetzung vorgeschlagener Maßnahmen

In der zweiten, überarbeiteten Datenschutz-Folgenabschätzung (DSFA) des Kultusministeriums vom 16. Oktober 2020 werden einige Maßnahmen zur Risiko-Minimierung vorgeschlagen. Auf Seite 103 steht dazu unter „Umsetzung der Abhilfemaßnahmen“:

> *Wir weisen darauf hin, dass bevor die geplante Datenverarbeitung implementiert wird – hier: Ausrollen der Software und entsprechende Kommunikation an die Schulen und Lehrkräfte –, müssen die für die Eindämmung des Risikos geeigneten und oben identifizierten Abhilfemaßnahmen ins Werk gesetzt sein.* ***Erst nach der Umsetzung darf die Verarbeitung personenbezogener Daten stattfinden.***
> (Hervorhebung nicht im Original)

Ungeachtet dessen, ob wir die geforderten Abhilfemaßnahmen als ausreichend bewerten stellt die folgende Tabelle den aktuellen Umsetzungsstand der auf Seite 84 der DSFA vorgeschlagenen technischen Maßnahmen aus unserer Sicht dar.

Abhilfemaßnahme	Stand der Umsetzung und Bemerkungen
Zwei-Faktor-Authentifizierungen	**Ist umgesetzt.** Im Rahmen des Pilotbetriebs konnte festgestellt werden, dass diese Abhilfemaßnahme aktiviert wurde. Allerdings war die Nutzung der MS Authenticator App anders als in der DSFA beschrieben (Seite 88) nicht deaktiviert (siehe Anlage *Analyse MS-Authenticator Android*).
Ende-zu-Ende-Verschlüsselungen	**Nicht umgesetzt.** Die umgesetzten Maßnahmen mittels OME stellen

Abhilfemaßnahme	Stand der Umsetzung und Bemerkungen
	keine Ende-zu-Ende-Verschlüsselung dar, sondern im Ergebnis nur eine Art erweiterte Transportverschlüsselung. Insbesondere schützen sie nicht vor Nach unserem Hinweis wurde zwar die Bezeichnung „Ende zu Ende Verschlüsselung“ im *Anhang 5 Fachkonzept Secure E-Mail Flow* angepasst, in der DSFA selbst wird als Abhilfemaßnahme Ende-zu-Ende-Verschlüsselung gefordert.
Protokollierung Dem KM soll ermöglicht werden, „den Zugriff der Lehrkräfte auf die dienstliche E- Mail-Adresse zur Gewährleistung von Datenschutz und IT-Sicherheit zu protokollieren“	**Unklar.** Welche genaue Protokollierung und welche Auswertungen stattfinden sollen und ob diese mit der DS-GVO vereinbar sind ist konnte im Rahmen des Pilotbetriebs durch den LfDI nicht umfassend geklärt werden. Die im *Anhang 6 Fachkonzept Governance* vorgeschlagenen Protokollierungen sind nur grob beschrieben. So stellt sich die Frage, welche Zugriffe im Detail protokolliert und geprüft werden soll, warum ein externer „Betriebspartner“ auf diese Daten Zugriff haben soll und unter welchen Bedingungen diese Zugriffe erfolgen können und dürfen.
privacy by default Laut DSFA: *Einstellung der Diagnosedaten durch den Verantwortlichen – nicht korrigierbar durch den Endnutzer – auf die Einstellung „Weder noch“. Verbleibend werden dadurch nur noch diejenigen Daten übermittelt, die die Wesentlichen Dienste betreffen.*	**Nicht umgesetzt.** Eine Übermittlung von Diagnose-, Telemetrie- oder anders genannten Daten der Nutzer durch das Kultusministerium an Microsoft sowie die eigennützige Weiterverarbeitung dieser Daten durch Microsoft im Wege der Beobachtung, Aufzeichnung und Auswertung des Nutzer- und Geräteverhaltens ohne erkennbare Rechtsgrundlage findet nach unseren Messungen im Rahmen des Pilotbetriebs weiterhin und in großem Umfang statt. Die Reduzierung der Übermittlung dieser Daten an Microsoft ist im Rahmen der Web-Versionen von MS 365 nach Angaben von Microsoft nicht möglich.

Abhilfemaßnahme	Stand der Umsetzung und Bemerkungen
	Zudem sind auch die Diagnosedaten, die von Microsoft in „Wesentliche Dienste“ umbenannt wurden, problematisch. Eine systematische Beschreibung und Analyse dieser Daten findet weder in der DSFA noch in den Begleitdokumenten statt.
Ausgestaltung des Vertrages mit dem Auftragsverarbeiter	
Normative Maßnahmen seitens des Kultusministeriums	**Teilweise umgesetzt** Nicht alle genannten Maßnahmen greifen; z.B. die „Zwingende Vorgaben der Verschlüsselung von Kommunikation und dienstlichen Arbeitsdaten“ greifen nicht, da der Dienst in der zumindest in der vorliegenden Konfiguration keine Möglichkeit Bietet, Daten vor dem Zugriff des Betreibers zu schützen. Der Ausschluss von besonderen Kategorien Personenbezogener Daten (Art. 9 DS-GVO) hat sich als nicht praktikabel erwiesen.

Demnach sind nicht alle in der Datenschutz-Folgenabschätzung des Ministeriums als unabdingbar angegebenen Abhilfemaßnahmen umgesetzt.