Maßnahmen für den datenschutzgerechten Einsatz von Microsoft 365

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) hat im November 2022 bereits zum zweiten Mal infrage gestellt, dass Microsoft 365 datenschutzkonform eingesetzt werden kann. Die eigentlich logische Konsequenz, den Einsatz zu verbieten, ziehen die Datenschutzbehörden allerdings nicht. Verantwortliche sind durch dieses Verhalten der Aufsichtsbehörden ein Stück weit auf sich gestellt und sollten im Rahmen einer Selbsteinschätzung über den Einsatz entscheiden. Nachfolgend stellen wir daher Maßnahmen vor, mit denen das Risiko des Einsatzes zumindest reduziert werden kann – gerade auch mit Blick auf das neue Angebot von Microsoft (EU Data Boundaries).

Das zentrale Problem beim Einsatz von Microsoft 365 (MS 365) ist, dass es sich bei den Programmen um komplexe Anwendungen handelt, in denen auf unterschiedliche Weise und von unterschiedlichen Akteuren Daten verarbeitet werden. Da es sich bei der Microsoft Gruppe um einen internationalen Konzern handelt, finden die Verarbeitungen zudem teilweise in Drittstaaten statt und potentiell in allen Ländern, in denen Microsoft tätig wird. Noch unübersichtlicher werden die Datenverarbeitungen dadurch, dass man als Kunde die Möglichkeit hat, innerhalb der MS 365-Anwendungen zahlreiche Tools von Drittanbietern zu verwenden, die wiederum Daten der Nutzer verarbeiten. Solche komplexen Anwendungen sind mit den Vorgaben des Datenschutzrechts schwer in Einklang zu bringen.

Problemübersicht

Datenschutzrechtlich problematisch sind insbesondere die folgenden Punkte:

- **Auftragsverarbeitungsvertrag**
  Für die Verwendung von MS 365 schließen der Kunde und die Microsoft Ireland Operations Limited (Microsoft) einen Auftragsverarbeitungsvertrag, den sogenannten

„Datenschutznachtrag zu den Produkten und Services von Microsoft“ (DPA) ab. Das DPA wird fortlaufend überarbeitet und erneuert. Die aktuellste Version datiert vom 01.01.2023 (Stand: 14.04.2023) und enthält einige Punkte, die insbesondere von der DSK kritisiert werden, nämlich:

- **Rechenschaftspflicht**
  Microsoft ermächtigt sich in dem DPA zur Verarbeitung sogenannter (ggf. personenbezogener) Telemetrie- und Diagnosedaten für eigene Zwecke in eigener Verantwortung. Telemetrie- und Diagnosedaten sind Metadaten, die bei der Verwendung von MS 365-Produkten generiert werden. Es ist nicht hinreichend eindeutig, welche Daten Microsoft dabei für eigene Zwecke verarbeitet. Die Verantwortlichen können daher ihre Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) nur unzureichend erfüllen.

- **Offenlegung von Daten**
  Microsoft behält sich die Offenlegungen von Daten gegenüber Behörden in Drittstaaten vor, falls Microsoft gesetzlich dazu gezwungen ist; dies widerspricht Art. 28 Abs. 3 S. 2 lit. a) DSGVO, der Datenverarbeitungen außerhalb der Weisungen des Verantwortlichen nur erlaubt, wenn das Recht der Union oder der Mitgliedstaaten die Verarbeitung vorschreibt.

- **Drittstaatentransfers**
  Microsoft behält sich vor, Daten aufgrund der Standardvertragsklauseln vom 04.06.2021 in alle Länder der Welt zu übermitteln, in denen Microsoft oder seine Unterauftragsverarbeiter tätig sind. Das ist eine große Zahl von Ländern, zu denen u.a. China, Indien, Marokko und andere Staaten gehören, in denen möglicherweise unverhältnismäßige Eingriffe in personenbezogene Daten vorgenommen werden können.

- **Rollenverteilung**
  Damit enthält bereits das von Microsoft verwendete DPA problematische Regelungen. Zusätzlich können bei der Anwendung von MS 365 Datenverarbeitungen erfolgen, die im DPA gar nicht erwähnt sind. So können aus MS 365-

Anwendungen heraus bspw. Suchaktionen mit Microsoft Bing durchgeführt werden. Dabei ist Microsoft Verantwortlicher für die Datenverarbeitung, nicht der Kunde. Im DPA ist dies nicht aufgeführt. Ebenso wenig genannt werden Datenverarbeitungen in der Verantwortlichkeit von Drittanbietern, die bspw. bei der Nutzung von Teams eingebunden werden können.

- **Überwachung/Profiling**
  Untersuchungen haben zudem ergeben, dass mithilfe von Telemetrie- und Diagnosedaten die Aktionen von Nutzern teilweise lückenlos nachvollzogen werden können. Es bestehen keine Anzeichen dafür, dass Microsoft von dieser Möglichkeit Gebrauch macht. Dennoch begründet sie ein hohes Risiko für die Persönlichkeitsrechte der Nutzer.

- **Überwachung von Mitarbeitern**
  Einige Funktionen (Viva Insights, Teams Analytics, ggf. auch der Diagnostic Data Viewer, Statusanzeige in Teams) ermöglichen bei entsprechender Verwendungsabsicht eine übermäßige Kontrolle von Arbeitnehmern, die MS 365-Anwendungen verwenden.

Diese und weitere Datenverarbeitungen machen die Verwendung von MS 365 problematisch. Verantwortliche stehen den Problemen allerdings nicht machtlos gegenüber. Durch eine datenschutzfreundliche Konfiguration der MS 365-Anwendungen und ggf. der IT-Umgebung können die Risiken reduziert werden.

Erforderliche Konfigurationen/Maßnahmen zur sicheren Verwendung von Microsoft

Nachfolgend benennen wir Maßnahmen, mit denen die Risiken des Einsatzes von MS 365 begrenzt werden können. Welche der Maßnahmen im Einzelfall erforderlich sind, hängt auch davon ab, welche Art von Daten ein Verantwortlicher in welchem Umfang verarbeitet. Eine Kindertagesstätte, in der sensible Daten von Kindern verarbeitet werden, muss sicherlich intensivere Maßnahmen ergreifen als bspw. ein Handelsunternehmen, das mit geschäftlichen Kontaktdaten von Ansprechpartnern arbeitet.

- **Auftragsverarbeitungsvertrag**
  Was zunächst die vertraglichen Mängel des DPA angeht, haben die meisten Kunden wohl nur sehr geringe Einwirkungsmöglichkeiten. Bei sehr großen, verhandlungsstarken Partnern von Microsoft kann es gelegentlich und im Ausnahmefall zu individuellen Vertragsanpassungen kommen. Den meisten Unternehmen wird aber regelmäßig nichts anderes übrigbleiben, als die Bedingungen zu akzeptieren. In diesem Fall bleiben den Verantwortlichen die folgenden Maßnahmen:

  - **Aktualisierung:** Unternehmen sollten zunächst darauf achten, dass immer das aktuellste von Microsoft zur Verfügung gestellte DPA Anwendung findet. Hierfür müssen Verantwortliche die Geltung der DPAs gesondert mit Microsoft oder ihrem Microsoft Partner vereinbaren. Ansonsten gilt das DPA, das im Zeitpunkt der letzten vertraglichen Änderung galt.

  - **Drittstaatentransfers:** Drittstaatenübermittlungen können teilweise durch die Verwendung der sogenannten EU Data Boundaries eingeschränkt werden. Bisher gilt das aber nicht für Telemetrie- und Diagnosedaten und für Professional Service Daten. Trotzdem führen die EU Data Boundaries schon jetzt zu einer erheblichen Risikominimierung. Voraussichtlich ab Anfang 2024 ist eine Nutzung von Microsoft vollständig ohne Datenübermittlungen in Drittstaaten möglich. Zusätzlich können sensible Daten durch eine Customer Lockbox verschlüsselt und so vor unbefugtem Zugriff gesichert werden.

  - **Auftragsverarbeitungsvertrag:** Darüber hinaus bleibt den Verantwortlichen in Bezug auf etwaige Mängel des DPA, insbesondere im Hinblick auf die Einhaltung ihrer Rechenschaftspflicht, nur, diese zu analysieren und anschließend eine Risikoabwägung zu treffen.

- **Rollenverteilung**
  Die Verarbeitung von Daten durch Microsoft und etwaige Drittanbieter in eigener Verantwortung kann mithilfe der

folgenden Maßnahmen und Konfigurationen eingeschränkt werden:

- Deaktivieren der verbundenen Dienste und Erfahrungen
- keine Integration von LinkedIn-Accounts der Nutzer
- keine Datenübermittlung zur Verbesserung der Benutzerfreundlichkeit
- Verbot von Drittanbieter Apps in Teams

- **Überwachung/Profiling**
  Eine unzulässige Ausforschung der Nutzer durch umfangreich erhobene Telemetrie- und Diagnosedaten kann mithilfe der folgenden Maßnahmen unterbunden werden:

  - Die Verwendung von **Telemetrie- und Diagnosedaten** durch Microsoft kann eingeschränkt werden, indem die Übermittlung hierfür auf „weder noch“ eingestellt wird. Zusätzlich kann die Übermittlung von Telemetriedaten auch mithilfe von technischen Maßnahmen eingeschränkt werden (Firewall), dies führt allerdings zu Funktionseinschränkungen bei der Verwendung von MS 365.

  - In mobilen Apps und Webversionen kann die Verarbeitung von **Telemetrie- und Diagnosedaten** durch Microsoft nicht eingeschränkt werden. Mobile Apps und Webversionen sollten daher nicht verwendet werden.

  - Welche Daten an Microsoft übermittelt werden, kann mithilfe des Diagnostic Data Viewers nachvollzogen werden.

- **Überwachung von Mitarbeitern**
  Die Verwendung von MS 365 darf nicht zu einer unzulässigen Ausforschung von Mitarbeitern führen. Dafür ist erforderlich:

  - keine Verwendung von Viva Insights, Teams Analytics, ggfs. auch der Statusanzeige bei Teams

  - kein Einsatz des Diagnostic Data Viewers, um Mitarbeiter unangemessen zu kontrollieren, dies kann

durch interne Organisationsvorgaben, die dies untersagen, sichergestellt werden

- Der Einsatz von MS 365 und die Verwendung zur Kontrolle von Mitarbeitern sollte mit dem Betriebsrat vereinbart und im Idealfall in einer Betriebsvereinbarung geregelt werden.

- **Sonstige Maßnahmen**
  Zusätzlich sollten E-Mails und 1:1-Telefonate per Teams verschlüsselt werden.

Datenschutz-Folgenabschätzung?

Verlässlich bewertet und zusätzlich abgesichert werden kann die Verwendung von MS 365, indem eine Datenschutz-Folgenabschätzung über die Verarbeitung von Daten mithilfe der Anwendungen durchgeführt wird. Ob dies rechtlich stets erforderlich ist, wird aktuell unterschiedlich bewertet. Nach einem jüngeren Urteil des LAG Rheinland-Pfalz vom 29.08.2022 (Az. 3 Sa 203/21, Rn. 61) begründet die Verarbeitung von Daten in einer MS 365-Cloud für sich genommen noch kein hohes Risiko für die Rechte und Freiheiten der Betroffenen. Eine Datenschutz-Folgenabschätzung ist demnach zumindest nicht bei allen Verantwortlichen obligatorisch. Je sensibler die Daten sind, die mithilfe der Anwendungen verarbeitet werden, desto eher ist aber eine Datenschutz-Folgenabschätzung erforderlich. Auch bei weniger sensiblen Daten kann sie helfen, die Risiken des Einsatzes von MS 365 korrekt einschätzen zu können.

Fazit

Der Einsatz von MS 365 birgt Risiken, die insbesondere mit den aufgeführten Maßnahmen reduziert werden können. Ein Restrisiko besteht daher auch bei einem kontrollierten Einsatz von MS 365. Über dieses Restrisiko muss eine informierte und bewusste Entscheidung getroffen werden.

Für alle weiteren Fragen rund um das Datenschutzrecht stehen Ihnen gerne zur Verfügung

Dr. Kristina Schreiber
+49(0)221 65065-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49(0)221 65065-200
simon.kohm@loschelder.de

Dr. Malte Göbel
+49(0)221 65065-337
malte.goebel@loschelder.de

Philipp Schoel
+49(0)221 65065-200
philipp.schoel@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de