Microsoft

Microsoft Business User Forum e.V. mbuf

Praktische Schritte hin zu einer DSGVO-konformen Nutzung von Microsoft 365

Ein Fragenkatalog zur individuellen gewissenhaften Beantwortung

Die hier erarbeiteten Fragestellungen zu vertraglichen Regelungen und sicheren Verfahren zur Verschlüsselung in Verbindung mit einem guten Verständnis, welche Daten wie und wo verarbeitet werden, helfen Ihnen, am Ende für den eigenen Prozess eine DSGVO-konforme Nutzung von Microsoft 365 belegen zu können. Lassen Sie sich auf die beschriebene Methodik ein!

1. Datenschutz-Folgenabschätzung

Führen Sie eine Datenschutz-Folgenabschätzung für die geplante Nutzung der Microsoft Dienste durch. Was Sie dafür wissen müssen:

- ☐ Welche Daten werden verarbeitet? Alle Daten mit personenbezogenem Inhalt müssen bekannt sein oder erkannt werden – auch wie lange diese Daten vorgehalten werden sollen oder müssen!
- ☐ Haben Sie eine Klassifizierung der Daten auf Basis der Verarbeitungstätigkeit vorgenommen?
- ☐ Wie ist die Nutzung geplant?
- ☐ Welchen Zweck hat die Verarbeitung?
- ☐ Können Daten auch in anonymisierter oder pseudonymisierter Form verarbeitet werden?
- ☐ Welche Applikationen sollen verwendet werden?
- ☐ Microsoft 365-Applikationen (Online, Desktop oder Mobile Devices)?
- ☐ Welche nicht-Microsoft-Applikationen werden eingesetzt?
- ☐ Welche grundsätzlichen Risiken birgt die Nutzung der eingesetzten Applikationen?
- ☐ Machen Sie bei Bedarf eine Risikoabschätzung.
- ☐ Stellen Sie die Wahrung der Rechte Betroffener sicher?

Eventuell stellen die Datenschutzbeauftragen Ihres Bundeslandes entsprechende Leitfäden und Templates bereit. Zum Beispiel: BayLfD: Datenschutz-Folgenabschätzung (DSFA) (datenschutz-bayern.de).

2. Analyse des Datenflusses

Für eine Datenschutz-Folgenabschätzung ist es erforderlich, den Datenfluss zu analysieren.

- ☐ Werden Informationen an Drittländer übertragen? (Adequacy decisions - How the EU determines if a non-EU country has an adequate level of data protection. (europa.eu))
- ☐ Sind datenschutzrelevante Informationen enthalten?
- ☐ Welche Schutzmaßnahmen müssen getroffen werden?
- ☐ Ist die Microsoft 365-Umgebung eine Single- oder Multi-Geo-Umgebung?
- ☐ Wo ist das Rechenzentrum für die Datenhaltung lokalisiert? Liegt es innerhalb der Europäischen Gemeinschaft oder in einem Drittland? Für die Einschätzung der DSGVO-konformen Nutzung ist es notwendig, den Speicherort der Kundendaten zu kennen. In Microsoft 365 kann die Lokation der Datenspeicher im Admin Center angezeigt werden.

Als Mitglied des Microsoft Business User Forum e.V. können Sie Ausarbeitungen über den Datenfluss der Applikationen Microsoft Teams oder Forms erhalten, weitere Applikationen sind in Arbeit. Sprechen Sie uns an: www.mbuf.de.

3. Sind die neuen Datenschutzbedingungen Bestandteil Ihres Vertrages?

Stellen Sie sicher, dass die aktuellen Datenschutzbestimmungen (Datenschutznachtrag zu den Produkten und Services von Microsoft - Letzte Aktualisierung: 15. September 2021) Bestandteil Ihres Vertrages mit Microsoft sind und für sämtliche Ihrer Microsoft Cloud-Abonnements gelten – auch für diejenigen, die in der Vergangenheit beschafft wurden. Sprechen Sie dazu Ihren Lizensierungspartner an.

4. Nutzen Sie individuelle Verschlüsselungen?

Einige Landesdatenschützer:innen sprechen die Empfehlung aus, Daten mit dem eigenen Schlüssel zu verschlüsseln. Dies kann innerhalb von Microsoft 365 mit einem Kundenschlüssel erreicht werden (Customer Key).

5. Haben Sie den Betriebsrat mit eingebunden?

Der Betriebsrat sollte bei Bedarf bereits in der Projektphase eingebunden werden.

- ☐ Haben Sie den Betriebsrat über die geplante Nutzung informiert?
- ☐ Wurde (falls Bedarf besteht) eine Nutzungsvereinbarung mit dem Betriebsrat erarbeitet?

Lassen Sie sich auf die beschriebene Methodik ein! Haben Sie die adressierten Fragen für Ihr Unternehmen gewissenhaft beantwortet, steht einer belastbaren Datenschutz-Folgenabschätzung nichts im Weg.