Datenschutzanalyse zu Miro

I. Zu bewertendes Verfahren/Tool und Zweckbestimmung

Miro ist ein Kommunikationstool bei dem mit Hilfe eines digitalen Whiteboards das Arbeiten in Teams und Projektgruppen vereinfacht werden soll. Der Nutzer erstellt ein Whiteboard und kann dann über dieses Whiteboard mit anderen Nutzern zusammenarbeiten. Der Anbieter, RealtimeBoard, Inc. dba Miro, kommt aus den USA und nutzt nach eigenen Angaben Server von Amazon (AWS) in Europa und in den USA. Miro sagt in einer Zusatzvereinbarung zum Datenschutz für den EU-Raum eine Speicherung in der EU zu und verweist auf einen eigenen Datenschutzbeauftragten in den Niederlanden.

1. Betroffenengruppen deren personenbezogene Daten verarbeitet werden

- Teilnehmende an der Whiteboardsitzung/Konferenz, sowohl Teilnehmende einer Bildungsmaßnahme als auch Dozierende und Mitarbeitende der Bildungseinrichtung.

2. Art der Daten

- Angaben zum/zur Benutzer*in: Bei Einrichtung eines Nutzerkontos Vor- und Nachname, E-Mail-Adresse - ansonsten auch ohne Benutzerangaben nutzbar. Für die Einrichtung ggfls. auch Daten zur finanziellen Abwicklung etc.
- Meeting-Metadaten: Nutzungsdaten und Cookies.

  Verwendete Nutzungsdaten u.a. die IP-Adresse, der Browsertyp, die aufgerufenen Seiten, die Nutzungsdauer und das Nutzungsdatum, die Geräte-ID und Diagnose-Daten. Bei der iOS App werden im App Store Zugriff auf Standortdaten, Nutzungsdaten, Diagnosedaten und Kennungen abgefragt.

  Miro verwendet nicht nur Session- und Sicherheitscookies, sondern auch tracking Cookies z.B. von Google Analytics und zwar auch beim Aufruf des Miroboards mit einem Einladungslink für nicht registrierte Nutzer*innen (zu Google Analytics nachfolgend unter 3.)

  In der Datenschutzerklärung wird auf eigene Cookies und Cookies und tracking Pixel (Bacon) von nicht näher spezifizierten Dienstleistern für Miro hingewiesen.

Gefördert vom
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

3. An der Verarbeitung beteiligten Komponenten (Systeme und Dienste sowie Prozesse)

Miro hat nach eigenen Angaben mehrere Trackingtools im Einsatz, wovon nur Google Analytics benannt wird. Nach Angaben von Miro sind Daten, die über Google Analytics erhoben werden anonymisiert. Eine Überprüfung zur IP-Anonymisierung ergab, dass im konkreten Fall keine Anfrage an Google geschickt wurde, die Internetseite aber grundsätzlich Tracker ohne IP-Anonymisierung einsetzt (Google Analytics-Prüfung der Universität Bamberg).
In der Cookierichtlinie teilt Miro zudem mit, dass sie selbst weitere nicht näher benannte Cookies nutzen, ohne das der Nutzer ein Konto bei Miro hat. In der Analyse mit Webbkoll DataSkydd lassen sich zahlreiche Kontakte zu weiteren Diensten nachweisen, die meisten davon in den USA. Bei Aufruf der Miro Seite werden 48 Cookies registriert, davon 19 von Drittanbietern.
Ob zumindest Miro – wie behauptet - die Daten ausschließlich auf Servern in der EU speichert, lässt sich nicht abschließend klären. In einer aktuellen Antwort (September 2021) auf die Frage der Speicherung, teilte Miro mit, dass die Daten in der EU und in den USA gespeichert werden, aber die DSGVO auf jeden Fall eingehalten wird.
Miro teilt zudem mit, dass sie nicht auf „Do Not track“- Signale reagieren.
Bezüglich der iOS App werden im App Store Zugriff auf Standortdaten, Nutzungsdaten, Diagnosedaten und Kennungen als Daten angegeben, die über die App abfließen (siehe https://datenschutz-schule.info/datenschutz-check/miro-board-online-whiteboard/).

II. Schutzbedarfsbestimmung

Gewährleistungsziele:
hier insbesondere Integrität / Vertraulichkeit / Nichtverkettung / Transparenz / Intervenierbarkeit.
Schadenshöhe:

Gefördert vom
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

Gering: Bei den Nutzerdaten handelt es sich um personenbezogene Daten, deren missbräuchliche Verarbeitung keine besonders schwerwiegende Beeinträchtigung des Betroffenen erwarten lässt.

Normal:

Bei den Metadaten handelt sich um personenbezogene Daten, deren missbräuchliche Verarbeitung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann. Dies umso mehr, als der Datenabfluss z.B. auch Standortdaten erfasst.

Hoch:

Sehr hoch:

III. Ermittlung von Gefährdungen/Bedrohungen für die Verfahrenskomponenten

Bedrohungen werden anhand des Gefährdungskatalogs (IT Grundschutz-Kompendium) ermittelt.

1. Aus der Gestaltung der Verarbeitungstätigkeit

Miro bietet eine kostenlose Schulvariante an, für die allerdings nicht sämtliche Vertragsvereinbarungen gelten. Mit Abschluss einer Schullizenz erhält man allerdings eine Zusatzvereinbarung zum Datenschutz (Data Processing Addendum), die auf die bestehende EU-Gesetzeslage Bezug nimmt und sich aktuell seit dem 29.September 2021 auf die Standardschutzklauseln EU-Vereinigtes Königreich beziehen.

2. Aus dem Bereich IT Sicherheit und dem organisatorischen Umfeld der Verarbeitung

Unterstellt die Daten von EU Nutzern werden auch in der EU gespeichert, gibt es dennoch diverse Abflüsse von Daten über die von Miro gesetzten Cookies und über die der Drittanbieter. Ob dabei personenbezogene Daten abfließen, inwieweit die in den USA verarbeitet werden und in welcher Art die Drittanbieter die Daten nutzen, ist schwierig zu ermitteln, weil Miro an der Stelle sehr ungenau wird und damit ein Risiko für das Gewährleistungsziel der Transparenz besteht.

Auch anonyme Nutzer (Teilnehmende), die ohne eigenes Nutzerkonto auf ein Miroboard zugreifen, werden über verschiedene Trackingtools verfolgt.

Gefördert vom
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

Trackingtools dienen üblicherweise auch dazu Metadaten zu personifizieren und mit den bisherigen Erkenntnissen über die IP - und die dahinterstehende Person - abzugleichen. Das stellt ein Risiko für die Vertraulichkeit, Nichtverkettung und Intervenierbarkeit dar.

IV Bewertung der Eintrittswahrscheinlichkeit

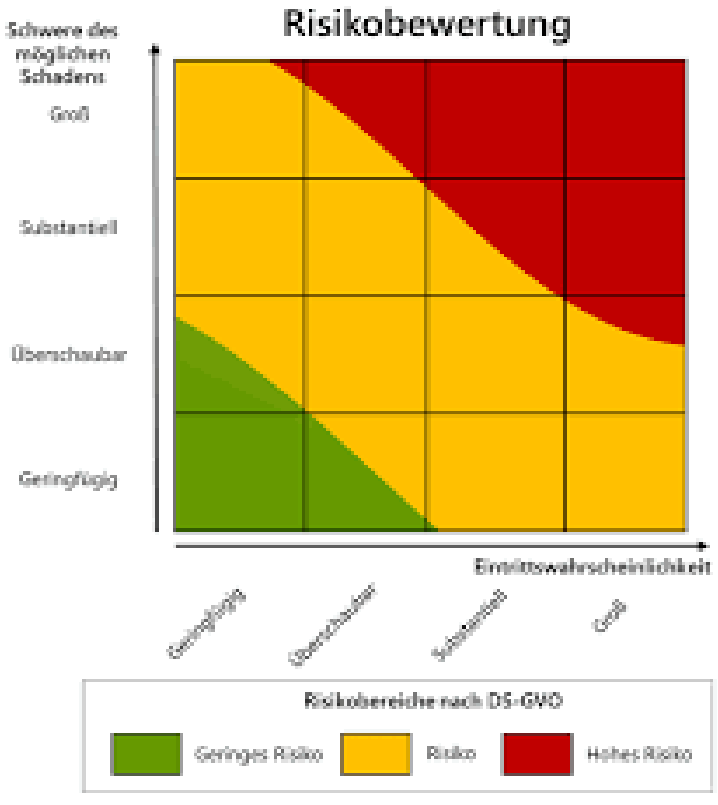
Äußerst selten:

Selten:

Gelegentlich:

Häufig: Konkrete Angaben können nicht gemacht werden. Allerdings können Tatsachen wie die, dass selbst anonyme Nutzer getrackt werden, als Indizien gewertet werden. Wenn es um die Frage des Datenabflusses geht, ist Miro intransparent. Es ist an dieser Stelle nicht abwegig von einer hohen Eintrittswahrscheinlichkeit von Risiken für die Gewährleistungsziele der Vertraulichkeit, der Nichtverkettung und der Transparenz durch Miro insbesondere aber durch die Drittanbieter auszugehen.

Bewertung:



Geringer bis normaler Schutzbedarf bei möglicherweise häufigem Eintritt einer missbräuchlichen Verwendung.

Gefördert vom
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

V. Auswertung:

Durch die Trackingtools besteht die Möglichkeit, dass die Metadaten der Nutzer bei nicht näher spezifizierten Dritten genutzt werden. Der dadurch entstehende Schaden kann – mangels Transparenz hinsichtlich der Trackingtools – nicht konkret benannt werden. Der Einsatz von Trackingtools selbst bei anonymen Nutzern und der wenig transparente Umgang damit, machen es schwierig, von einem noch akzeptablen Risiko zu sprechen.
Gegen eine Nutzung von Miro ausschließlich auf Endgeräten einer Bildungseinrichtung bestehen keine Bedenken.
Etwas anderes gilt hinsichtlich des Risikos, dem diejenigen ausgesetzt sind, die Miro mit privaten Endgeräten nutzen. Das Risiko lässt sich zwar technisch durch den Einsatz eines entsprechenden (kostenlosen) Browser-AddOn wie z.B. „AdGuard“ minimieren. Hierzu müsste den Teilnehmenden mitgeteilt werden, dass auch bei der anonymen Nutzung von Miro diverse Trackingtools eingesetzt werden und sich diejenigen, die nicht getrackt werden möchten, ein entsprechendes AddOn auf das eigene Endgerät installieren sollten. Ob damit aber auch alle Tracker erfasst werden, lässt sich nur mit erheblichem Arbeitsaufwand feststellen. Da Miro zudem mitteilt auf „do not track“ - Signale nicht zu reagieren, müsste eine intensive Auseinandersetzung mit der Frage der Eignung des zu nutzenden Browser-AddOn erfolgen.

Endergebnis: Miro ist – trotz der Beteuerung sich an die europäischen Datenschutzgesetze zu halten - im Hinblick auf den Einsatz von Trackingtools intransparent. Die Datenverarbeitung erfolgt nach eigenen Angaben in der EU und in den USA und es ist nicht eindeutig zu klären, ob Daten von EU Bürgern auch nur in der EU gespeichert werden. Ob, wie und wo die Drittanbieter die über den Cookie-Einsatz erlangten Daten verarbeiten, lässt sich nicht nachvollziehen. Zwar bezieht sich Miro seit der letzten Aktualisierung vom 29.09.2021 auf die Standardvertragsklauseln zwischen der EU und dem vereinigten Königreich, die aber keine Rechtsgrundlage für den wahrscheinlichen Datenabfluss in die USA darstellen.

Gefördert vom
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

Dem Gebrauch von Miro ausschließlich auf Endgeräten der Bildungseinrichtung stehen keine Bedenken entgegen. Der Gebrauch mit privaten Endgeräten begegnet Bedenken. Diese lassen sich dadurch minimieren, dass den Betroffenen aktiv zur Installation eines entsprechenden AddOn geraten wird. Zuvor muss das AddOn auf die Geeignetheit überprüft werden.

Zumindest für Bildungseinrichtungen, die Maßnahmen nach dem SGB durchführen oder aus anderen Gründen mit besonders schützenswerten Daten umgehen, ist vom Einsatz des Miro-Tools abzuraten.

Anmerkung: Der notwendige Auftragsdatenverarbeitungsvertrag wird bei Miro durch den sog. Data Processing Addendum erfüllt.

Gefördert vom
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen