

# DAB Digitalagentur Berlin

Digital Dip XR: XR trifft Digitalagentur Berlin  
Donnerstag, 27. Januar 2022



# Gemeinsam für Berlin

**Als zentrale Koordinierungsstelle werden wir gemeinsam mit allen Stakeholdern die Digitalisierung vorantreiben und Berlin nachhaltig zukunftsfähig machen. Die DAB unterstützt die Berliner Unternehmen in jeder Phase ihrer digitalen Transformation.**

100-prozentige Tochtergesellschaft der IBB Unternehmensverwaltung AöR sowie gefördert und finanziert vom Land Berlin.



# Gemeinsam für Berlin

## Unsere Aufgaben

- Zentrale Koordinierungs- und Anlaufstelle in Berlin für das Thema Digitalisierung
- Berliner Unternehmen für digitale Themen sensibilisieren
- Verständliche Aufbereitung der Digitalisierungsthemen
- Beratungs- und Unterstützungsangebote transparent und einfacher nutzbar machen
- Anlaufstelle für das Thema IT-Sicherheit
- Schnittstelle in die Berliner Verwaltung
- Ergänzung der Angebote bestehender Akteur\*innen und Verbindung zu diesen schaffen
- Wir bieten Austausch und Vernetzung an.



# Stakeholder der Digitalagentur Berlin



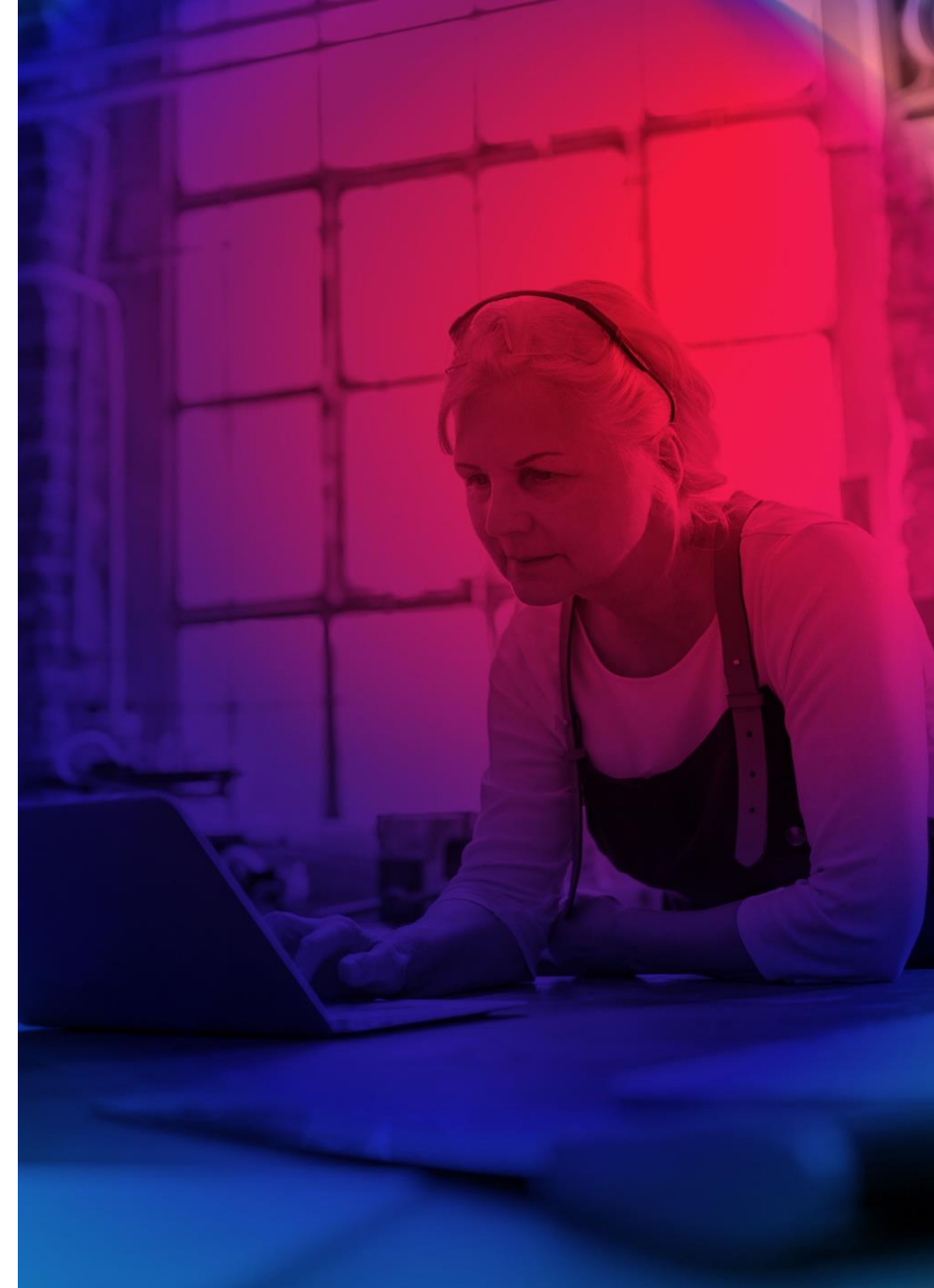
# Kund\*innen im Fokus

Wie und wo beginne ich meine digitale Reise?

Muss ich überhaupt digitalisieren? Warum nicht einfach „Weiter so?“

Welche Förderprogramme gibt es und wer kann mir bei meinem Vorhaben helfen?

**Fazit: Wir unterstützen Sie sehr gern auf Ihrer digitalen Reise in die Zukunft – gemeinsam, partnerschaftlich, verständlich und bedarfsorientiert.**



# Unsere Angebote

## Information zu Fördermöglichkeiten

Es gibt eine Vielzahl an Förder- und Finanzierungsangeboten vom Bund, Berlin und der EU: Wir helfen Ihnen, die Angebote zu sortieren und zu bewerten - angepasst für Ihr Digitalisierungsvorhaben.

## IT-Sicherheit

Die Basis für eine erfolgreiche Digitalisierung - Wir möchten Berliner Unternehmen sensibilisieren und erklären, wie der Einsatz von Standardsoftware und modernen Tools Sicherheitsrisiken reduzieren und Ihr Unternehmen besser schützen und damit wettbewerbsfähig machen kann.

## Formate

Wir vermitteln gern zu bestehenden Formaten unserer Netzwerkpartner\*innen und kreieren neue und gemeinsame Formate für die Berliner Unternehmen, die die vielfältigen Themen der Digitalisierung greifbar und umsetzbar machen.

# Unsere IT-Sicherheits-Angebote

## IT-Sicherheitskooperationspartner

- vermitteln bedarfsgenauer IT-Sicherheitspartner\*innen und Services an Berliner Unternehmen für Spezialgebiete und/oder weitere Betreuung

## IT-Sicherheitssupport

- zum Sensibilisieren und Informieren von Berliner Unternehmen auf Basis aktueller IT-Sicherheits-Normen
- über IT-Sicherheitsmaßnahmen
- für die Anwendung unserer DAB-ITS-Checklisten an Berliner Unternehmen

## IT-Sicherheitsseminare und -Webinare

- Seminare zu IT-Sicherheitsgrundlagen (z. B. ISO 27001) sowie „Best Practise“ für deren Umsetzung
- informieren Berliner Unternehmen über aktuelle IT-Sicherheitsthemen

# Unsere IT-Sicherheits-Angebote

## Aktuelle Gefährdungen

- Überblick über aktuelle IT-Sicherheits-Gefährdungen

## IT-Sicherheits-checklisten

- für wesentliche IT-Elemente
- unterstützen vollumfängliche IT-Sicherheit in Berliner Unternehmen

## IT-Sicherheits-hotline

- Telefon-Hotline für IT-Sicherheitsnotfälle und Anfragen

## IT-Sicherheit & DSGVO

- erläutern den Berliner Unternehmen die Datenschutz-Grundverordnung, die mit IT-Sicherheit zusammenhängt



# Chancen durch XR für die IT-Sicherheit

**Die Anwendung von XR in einem Unternehmen hat Vorteile für die IT-Sicherheit:**

- Visualisierung von Risiken und Bedrohungen
- VR-basierte Trainings zu: Homeoffice, Passwortsicherheit, mobiles Arbeiten, Phishing
- Einsatz in der IT-Forensik
- Kombination von VR, AR und Gaming zur Entscheidungsfindung in IT-Sicherheitsfragen

# Beachtung von DSGVO und IT-Sicherheit beim Einsatz von AR

## Beispiel für Einsatzmöglichkeiten von AR in Unternehmen:

Unternehmensbereich	Einsatz AR-Brille
„Marketing/ Verkauf“	Verkaufsunterstützung im Handel, z.B. AR mit Produktinformationen
„Produktion“	Zeiteffizientere und Risiko-verminderte Wartung und Reparatur, z.B. Anlagen

- Vor AR-Nutzung ist eine IT-Sicherheitsanalyse sowie eine Datenschutzfolgenabschätzung im Sinne der DSGVO durchzuführen
- AR-Datenspeicherung (Audio/Video) muss innerhalb der EU stattfinden
- Technische & Organisatorische Maßnahmen umsetzen, Art. 32 DSGVO z.B. Anonymisierung, Vertraulichkeit und Verfügbarkeit der AR-Systeme

# Augmented Reality (AR) & IT-Sicherheit

- Zur grundlegenden Prüfung der IT-Sicherheit können IT-Sicherheits- Checklisten der DAB Digitalagentur Berlin genutzt werden.
- Beispielhafte Maßnahmen zur IT-Sicherheit für Augmented Reality (AR)

Nr.	DAB IT-Sicherheitscheckliste Software: Schwachstellenanalyse und Maßnahmen
1	Nutzung eines Berechtigungs-Konzeptes auch für Augmented Reality (AR)
2	Absicherung von AR-Software auch mit Firewall und Anti-Virus-Produkten
3	Regelmäßige Einspielung von Patches und Softwareupdates

## IT-Sicherheitscheckliste

Software: Schwachstellenanalyse und Maßnahmen



Prüfen Sie an Hand der folgenden 10 Fragen, wie Ihr Unternehmen in Bezug auf IT-Sicherheit aufgestellt ist. Wenn Sie eine Frage mit **Nein** beantworten, haben wir für Sie Maßnahmen benannt, mit denen Sie Ihre IT-Sicherheit verbessern können.

IT-Sicherheitsfrage	Ja	Nein	Mögliche Maßnahme
1. Besteht eine Softwareübersicht oder -landschaft?	<input type="checkbox"/>	<input type="checkbox"/>	<ul style="list-style-type: none"> <li>› Erstellung einer Softwareübersicht (Kategorisierung der IT-Software etc.)</li> <li>› Visualisierung der IT- Softwarelandschaft</li> </ul>
2. Gibt es ein sicheres, einheitliches Installationsvorgehen für Software?	<input type="checkbox"/>	<input type="checkbox"/>	Die Installation von Software sollte nur von Befugten standardisiert und IT-sicher durchgeführt werden.
3. Wird regelmäßig kontrolliert, dass Nutzer*innen nur Zugriff auf die IT-Software haben, die berechtigt sind?	<input type="checkbox"/>	<input type="checkbox"/>	Regelmäßiges Software-Monitoring wird empfohlen (z.B. monatliche Berechtigungs-kontrolle).
4. Kennwörterverwaltung: werden starke Kennwörter systemseitig sichergestellt?	<input type="checkbox"/>	<input type="checkbox"/>	Vorhandene Passwortregeln sollten in der IT-Software eingestellt werden für die IT-Nutzer*innen: <ul style="list-style-type: none"> <li>› Passwörter sollten mindestens 8-stellig sein.</li> <li>› Verwenden Sie keine leicht zu erratene „Wörter“, sondern Sonderzeichen, Groß-/ Kleinbuchstaben und Zahlen als Passwort.</li> <li>› Verwenden Sie NIE das gleiche Passwort mehrmals.</li> </ul>
5. Wurden IT-Änderungen in Systemen oder in der Software vor der Produktivsetzung getestet?	<input type="checkbox"/>	<input type="checkbox"/>	Z. B. Tests: Systemabnahmetests, User Acceptance Tests, Systemsicherheitstests, Performancetests etc.
6. Ist ausgeschlossen, dass Software ohne Genehmigung geändert werden kann?	<input type="checkbox"/>	<input type="checkbox"/>	Funktionstrennung zwischen Entwickler*in, Administrator*in und IT-Anwender*in
7. Wird die Antivirus-Software und Firewall regelmäßig aktualisiert?	<input type="checkbox"/>	<input type="checkbox"/>	Jede*r Nutzer*in sollte seine*ihre Anti-virus-Software regelmäßig updaten.
8. Schauen Sie regelmäßig nach Updates und Patches für Ihre Software und spielen Sie diese ein?	<input type="checkbox"/>	<input type="checkbox"/>	Die IT sollte über aktuelle Patches informiert sein und diese bei Bedarf einspielen.
9. Gibt es ein regelmäßiges Backup für die Daten der Software?	<input type="checkbox"/>	<input type="checkbox"/>	Bestenfalls wird ein tägliches Backup aller Daten durchgeführt.
10. Findet eine DSGVO-konforme Ereignisprotokollierung in den IT-Systemen statt?	<input type="checkbox"/>	<input type="checkbox"/>	Protokolle sind in Systemen anzuschalten oder es ist eine protokollierende, DSGVO-konforme Software einzusetzen. Alternativ kann eine IT-Nutzer*innen-Historie im System hinterlegt werden, z. B. für Revisionszwecke.

Gerne unterstützen wir Sie bei der Umsetzung der Maßnahmen zur Erhöhung der IT-Sicherheit in Ihrem Unternehmen. Wir freuen uns auf Ihre Anfrage an [info@digitalagentur.berlin](mailto:info@digitalagentur.berlin).

Weitere Informationen finden Sie auch auf [digitalagentur.berlin](http://digitalagentur.berlin).

# Ihre Ansprechpartner



**Thomas Medl**

Projektmanager IT-Sicherheit

+49 (178) 573 32 85

Thomas.medl@digitalagentur.berlin



**Aylin Evin Citak**

Projekt- und Leadmanagerin

+49 (178) 574 47 28

Aylin.citak@digitalagentur.berlin