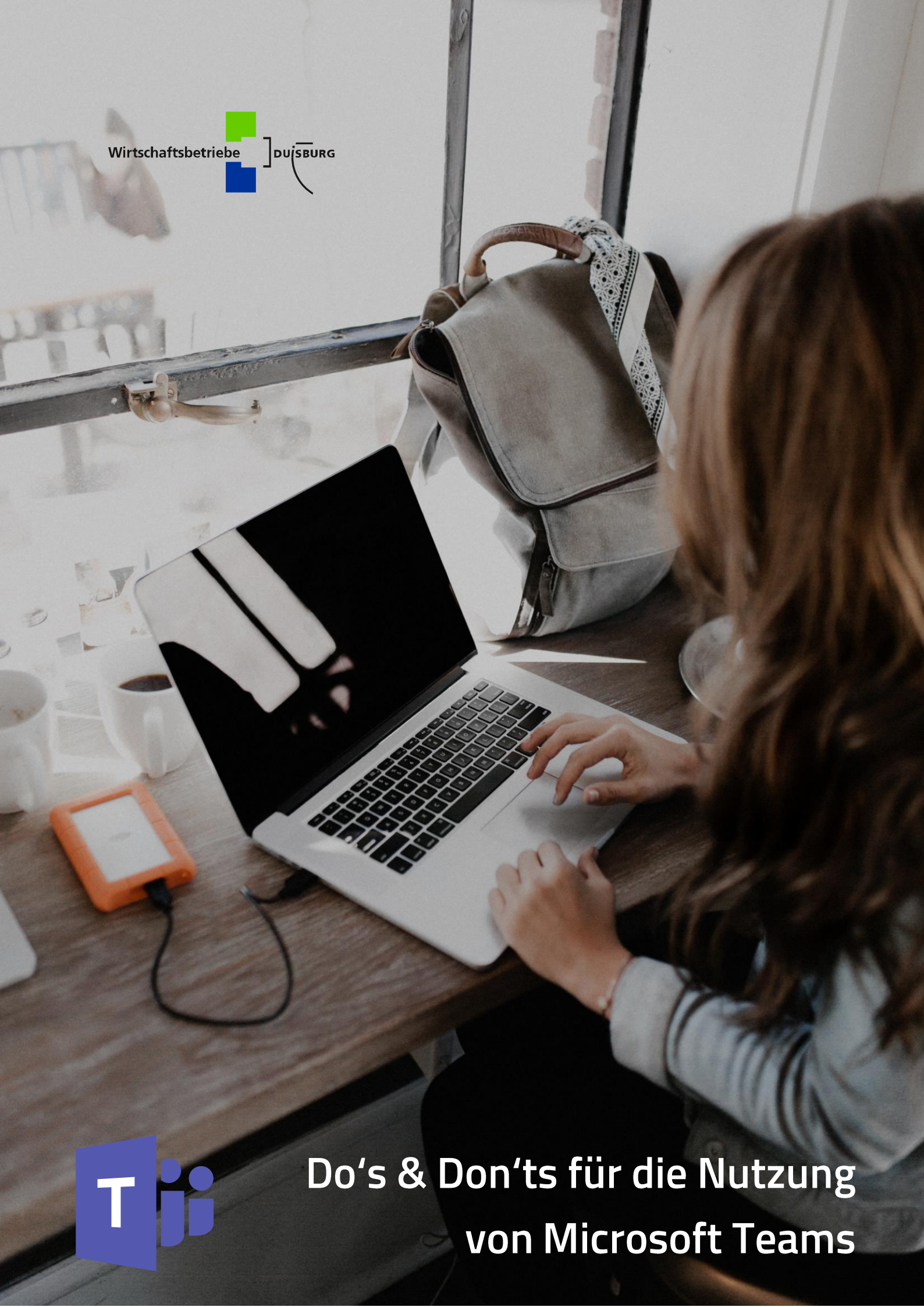

Wirtschaftsbetriebe DUISBURG

Do‘s & Don‘ts für die Nutzung von Microsoft Teams

EINLEITUNG

Mit der Einführung von **Microsoft Teams** bei der WBD-AöR ergeben sich sowohl für das Unternehmen, als auch die Beschäftigten **Chancen**, verschiedene Prozesse sowie die Kommunikation effizienter zu gestalten.

Damit die Kommunikation und Prozesse zusätzlich auch noch **sicher** ablaufen, wurden einige Aspekte für Sie in Form einer **„Do's/Check/Don'ts"-Liste** übersichtlich zusammengestellt. Die Kriterien in dieser Liste sollten bei der Nutzung von Microsoft Teams beachtet werden. Sie schützen sich und das Unternehmen dadurch unter anderem vor **Datenschutzverletzungen**. Ferner kann somit ein ausreichendes Maß an **IT-Sicherheit** gewährleistet werden.

Die nachfolgende Liste bezieht sich dabei primär auf die **WBD-interne Nutzung**, treffen aber z.B. auch auf (einmalige) Videokonferenzen und Sprachanrufe mit Dritten zu. Wenn **externe Dritte** als „längerfristige" Mitglieder in eine Teams-Gruppe aufgenommen werden sollen, ist zu prüfen, ob mit den jeweiligen Firmen Vertraulichkeitsvereinbarungen und ggf. Auftragsdatenverarbeitungsverträge bestehen, oder ob wesentliche Gründe gegen die Aufnahme in das Team sprechen.

Beachten Sie auch, dass die Inhalte der Registerkarten **„Beiträge", „Dateien" und „Wiki"** jeweils von allen Mitgliedern eines Teams bzw. (privaten) Kanals abrufbar sind!

Bei Fragen oder Anmerkungen, können Sie gerne die am Ende des Dokuments stehenden **Ansprechpersonen** kontaktieren.

Vielen Dank für die Berücksichtigung!

LEGENDE

Do's (Machen!)

Diese Dinge sind grundsätzlich zu empfehlen oder zu befolgen.

Check (Prüfen!)

Diese Sachverhalte sind im Einzelfall sorgfältig zu prüfen und abzuwägen.

Don'ts (Lassen!)

Diese Dinge müssen unterlassen werden.

Do‘s (Machen!)

Compliance-Grundsätze

- Gesetze
- interne Regelungen
- Unternehmenskultur/ „Netiquette“
- Kommunikationsleitfaden für die WBD-AöR

beachten.

Datenschutz-Grundsätze

Grundsätze der

- Datenminimierung
- Rechtmäßigkeit
- Zweckbindung
- Speicherbegrenzung
- Gesetze
- interne Regelungen

einhalten.

IT-Sicherheits-Grundsätze

- Dateien und Anhänge nur verschlüsselt versenden (lieber auf E-Mail/ Laufwerk V: ausweichen)
- Passwort über einen anderen Kanal übertragen (z.B. Telefonanruf)

Sprachanrufe & Chats

- Einzel- oder Gruppengespräche initiieren oder an solchen teilnehmen
- Neue Chats starten oder an Chats teilnehmen

Check (Prüfen!)

Compliance-Grundsätze

Interne Vorgaben in

- Arbeits- oder Verfahrensanweisung
- Dienstvereinbarung
- Kommunikationsleitfaden für die WBD-AöR

prüfen (Check: MHB, Intranet).

Datenschutz-Grundsätze

Grundsätzlich erlaubt ist das Einstellen von

- Vor- und Nachnamen,
- dienstlichen Kontaktdaten

Check: Notwendigkeit

IT-Sicherheits-Grundsätze

- Rücksprache halten mit Personen, die nicht angeforderte Dateien zusenden
- Dateien per E-Mail versenden bzw. über Laufwerk V: verteilen, anstatt über Teams

Sprachanrufe & Chats

Auf den Teilnehmerkreis achten Check: Berechtigungen; Welche Informationen werden geteilt oder habe ich vor zu teilen?

Hinweis: Auch nachträglich Eingeladene können den gesamten Chatverlauf einsehen!

Don’ts (Lassen!)

Compliance-Grundsätze

Gegen Vorschriften verstoßen.

Datenschutz-Grundsätze

Sensible personenbezogene Daten* oder Betriebs- oder Geschäftsgeheimnisse über Teams bearbeiten

IT-Sicherheits-Grundsätze

- Dateien von unbekannten Personen annehmen/öffnen
- Dateien unverschlüsselt über Teams versenden
- Passwörter übertragen

Sprachanrufe & Chats

Weitergabe von vertraulichen Informationen, Betriebs- oder Geschäftsgeheimnissen und sensiblen personenbezogenen Daten

* Insbesondere: Rassische**/ Ethnische Herkunft, politische Meinungen, religiöse/ weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische und biometrische Daten, Gesundheitsdaten, Daten zum Sexualleben oder zur sexuellen Orientierung.
** Zum Wortsinn des Begriffs s. VA – A 49 Ziff. 3.1.1.

Do's (Machen!)

Video-/Web-Konferenz

Gemeinsam Konferenzen abhalten - mit oder ohne Nutzung der Kamera

Bildschirm teilen

Konferenzteilnehmer/-innen auf das notwendige Maß begrenzen

Dateien teilen

Dateien ohne
- personenbezogene Daten
- „normale" dienstliche Informationen

über
- Bildschirmfreigabe oder Chat
- Dateien oder Wiki

gemeinsam bearbeiten.

Dateien speichern/ archivieren

Vorübergehendes Einstellen von gemeinsam zu bearbeitenden Dateien, die weder personenbezogene Daten noch Betriebs- und Geschäftsgeheimnisse beinhalten

Check (Prüfen!)

Video-/Web-Konferenz

Einschalten der Kamera bleibt jedem User selbst überlassen

Check: Selbstbestimmung

Hinweis: Den Hintergrund kann man verpixeln lassen oder durch ein Bild ersetzen.

Bildschirm teilen

Übertragung des gesamten Bildschirms erforderlich?

Check: Genügt das Teilen eines Fensters oder Programms?

Dateien teilen

Bei Dateien mit personenbezogenen Daten abwägen, ob eine gemeinsame Bearbeitung über
- Bildschirmfreigabe oder Chat
- Dateien oder Wiki

erfolgen sollte.

Check: Datenschutz-Grundsätze

Dateien speichern/ archivieren

Nicht mehr benötigte Dateien löschen

Check: Notwendigkeit

Don'ts (Lassen!)

Video-/Web-Konferenz

Druck aufbauen, damit Konferenzteil-nehmer/-innen die Kamera nutzen

Bildschirm teilen

Nicht Notwendiges übertragen

Hinweis: Outlook etc. schließen und Desktopsymbole ausblenden!

Dateien teilen

Dateien, die sensible personenbezogene Daten, Betriebs- und Geschäftsgeheimnisse oder vertrauliche Informationen enthalten,

in Teams

einstellen, bearbeiten oder speichern/ archivieren

Dateien speichern/ archivieren

Dateien dauerhaft speichern oder archivieren

Hinweis: Zum dauerhaften Speichern/ Archivieren Laufwerk V: oder Fachverfahren nutzen!

* Insbesondere: Rassische**/ Ethnische Herkunft, politische Meinungen, religiöse/ weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische und biometrische Daten, Gesundheitsdaten, Daten zum Sexualleben oder zur sexuellen Orientierung.
** Zum Wortsinn des Begriffs s. VA – A 49 Ziff. 3.1.1.

Wirtschaftsbetriebe DUISBURG

KONTAKT

Bei Fragen zu Microsoft Teams:

Roman Aiyer
Tel.: (0203) 283 - 7976
E-Mail: r.aiyer@wb-duisburg.de

Dr. David Hoffmann
Tel.: (0203) 283 - 2602
E-Mail: d.hoffmann@wb-duisburg.de

Bei allgemeinen Fragen zu den Themen Datenschutz, Datensicherheit und Compliance:

Martin Giesen
Tel.: (0203) 283 - 3506
E-Mail: m.giesen@wb-duisburg.de

Dennis Wienemann
Tel.: (0203) 283 - 2850
E-Mail: d.wienemann@wb-duisburg.de