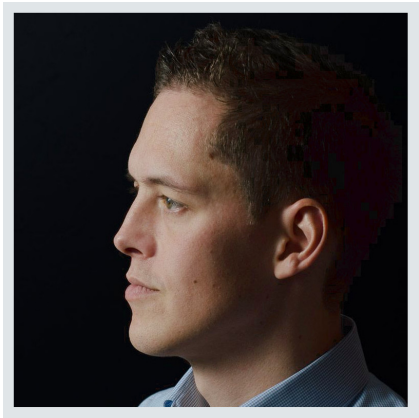
Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

WhatsApp-Alternativen: Eine Reise durch den Messenger-Dschungel

[29.04.2021] – Bildungszentrum Datenschutz und Informationsfreiheit Baden-Württemberg (BIDIB)

Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Zu meiner Person



Mike Kuketz

[1] 50% Tätigkeit beim LfDI (BW)

- Prüfung von Datenflüssen (insb. Android)
- Bearbeitung von technischen (Grundsatz-)Fragen
- Allgemein: (User-)Tracking, sicherheitsrelevante Themen

---

[2] IT-Security- / Datenschutz-Umfeld

- Mobile Security (Android, iOS)
- Daten-Analysen für Behörden, Journalisten etc.

[3] Blogger | Autor

- Blog: www.kuketz-blog.de | #IT-Sicherheit #Datenschutz
- Fachartikel: Computerzeitschrift c‘t

[4] Dozent | Referent

- Lehrbeauftragter »IT-Sicherheit« DHBW Karlsruhe

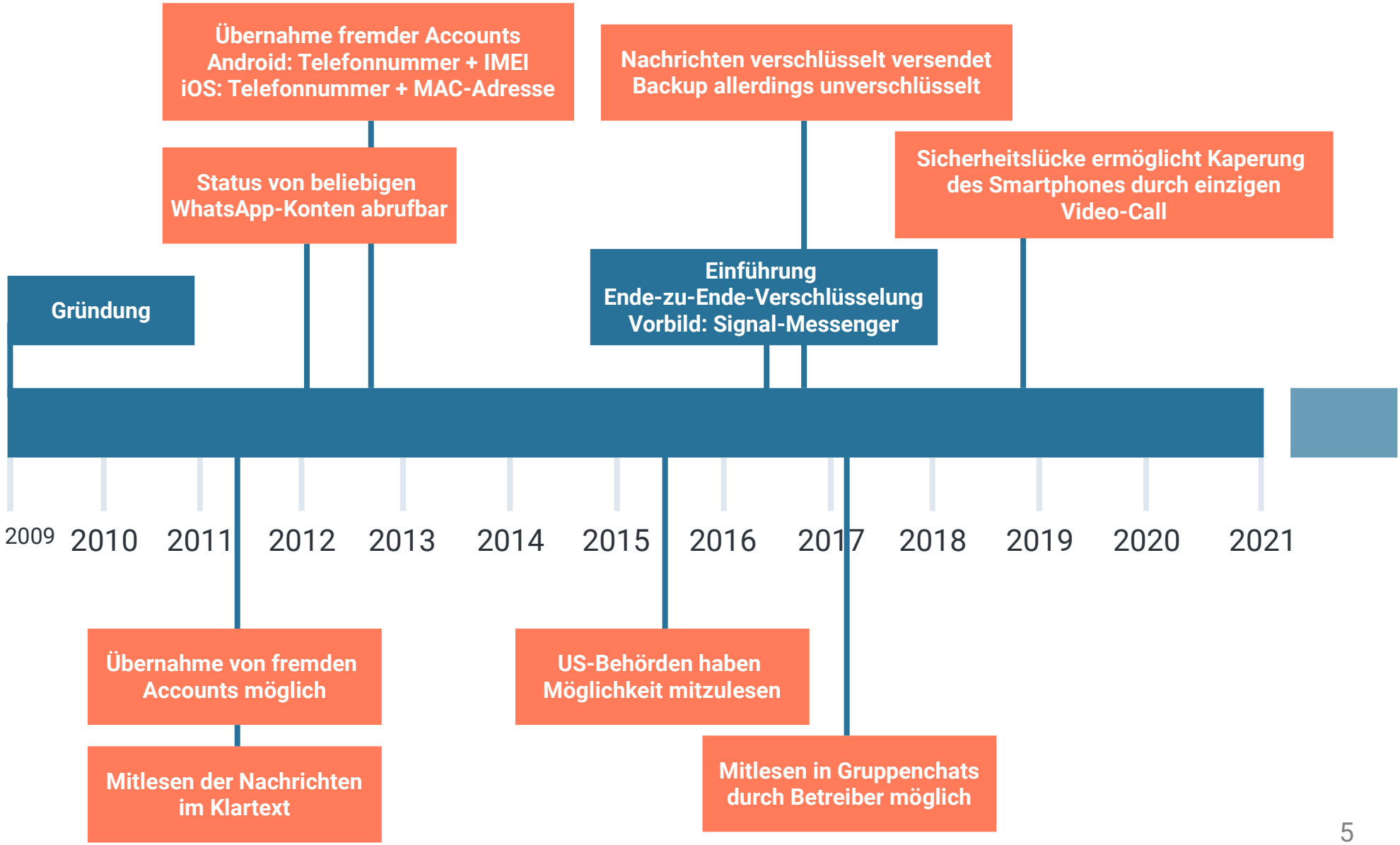
Agenda

- **[1]** WhatsApp
  - Ein Datenschutz- und Sicherheitsalbtraum
  - AGB-Änderungen: Was bedeutet das?
- **[2]** Bitte nicht vom Regen in die Traufe
  - Sichere und datenschutzfreundliche Messenger
- **[3]** Messenger: Zielgruppe und eigene Anforderungen/Bedürfnisse sind (mit-)entscheidend

1. Teil

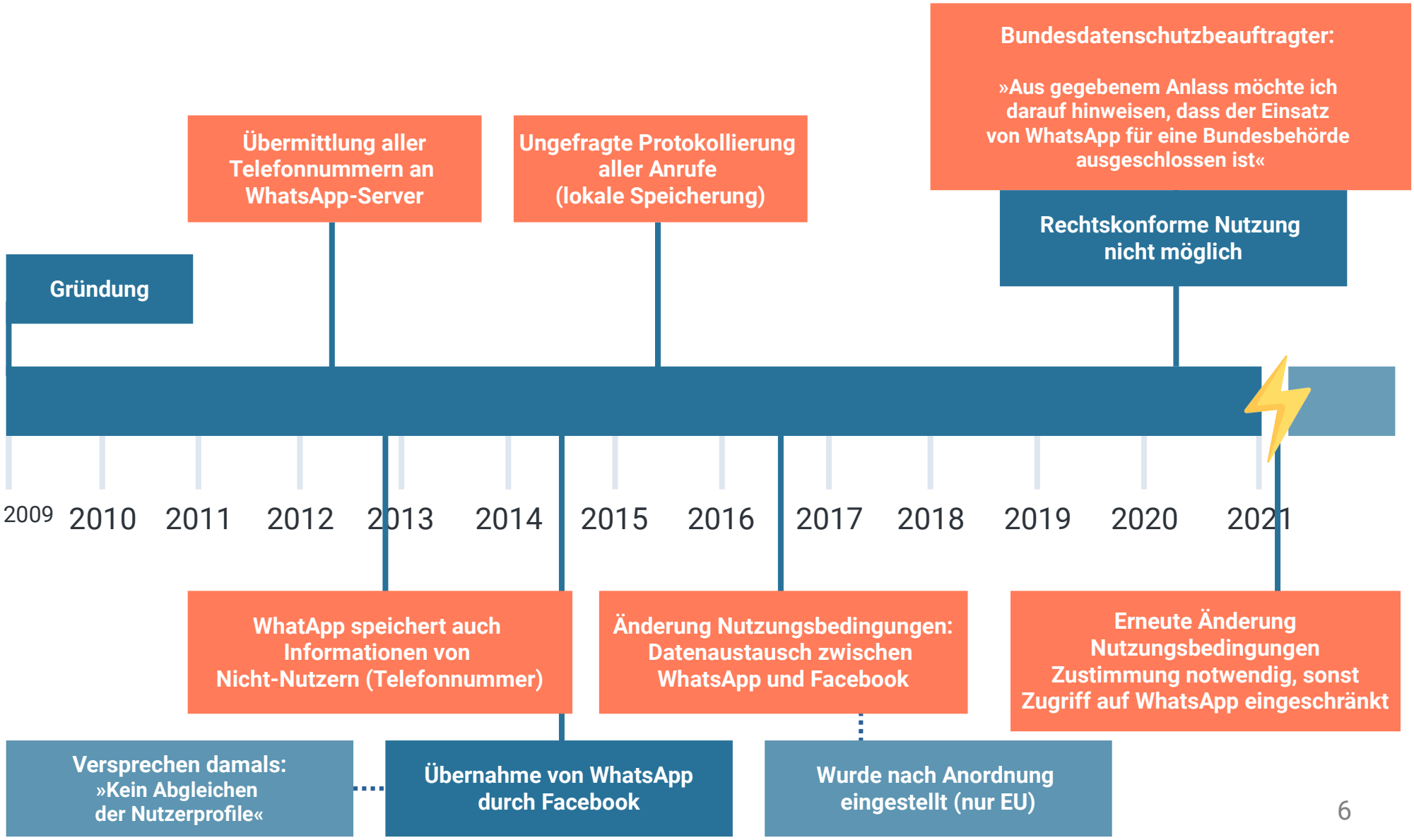
WhatsApp: Ein Datenschutz- und Sicherheitsalbtraum

[1] WhatsApp: Ein Rückblick (Sicherheit)



Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

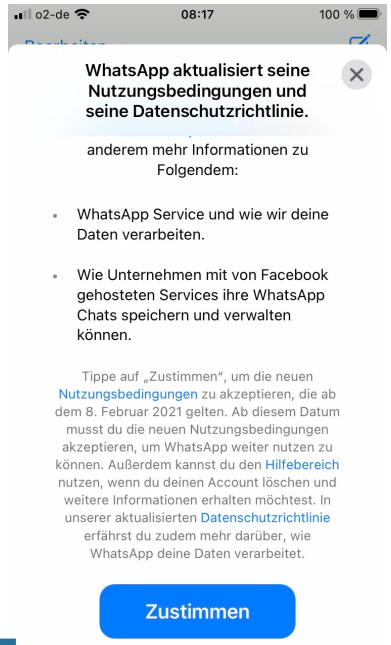
[2] WhatsApp: Ein Rückblick (Datenschutz)



Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

AGB: Zustimmung zur Datenweitergabe

- Stichtag 15. Mai 2021 für 2 Milliarden Nutzer (ehemals 8. Februar 2021)



Zwei Nutzungsbestimmungen

Nutzer in Europa

- WhatsApp erhält und teilt Informationen mit Facebook-Unternehmen (ähnlich 2018) – allerdings wohl keine Widerspruchmöglichkeit mehr
- schwammig/unklar welche Daten das konkret sind

Sonderregelung

Rest der Welt

- Verwendung der Nutzer-Informationen **auch** zu Facebook-Werbezwecken
- Die ehemalige Widerspruchsmöglichkeit wird also abgeschafft

Keine Auswahl mehr

(HmbBfDI) eröffnet Dringlichkeitsverfahren: Pauschale Einwilligung kann nichts rechtskonform sein

Welche Daten werden weitergegeben?

- Welche Daten konkret mit Facebook-(Unternehmen) geteilt werden ist unklar bzw. bleibt nebulös

- Wenn keine Zustimmung:
  - Konto wird nicht gesperrt
  - Allerdings eingeschränkte Nutzung
  - bspw. kein Senden/Empfangen von Nachrichten
  - Unklar, wie lange dieser »Zustand« anhält

(Meta-)Daten

- Verwendetes (mobiles) Gerät
- Betriebssystem
- Batteriestand
- Mobilfunkanbieter
- Telefonnummer
- Kontakte aus Adressbuch
- Profilbild
- Standortinformationen

[…]

WhatsApp löschen – aber richtig!

- Einfach die App löschen genügt nicht
- Beim Löschvorgang werden alle Chatverläufe und Backups gelöscht:
  - Einstellungen aufrufen
  - Account
  - »Meinen Account löschen« auswählen
  - Löschung mit Eingabe der Telefonnummer bestätigen

- Backup auf PC anfertigen
  - https://web.whatsapp.com - Verknüpfung WhatsApp mit Browser
  - Chrome Browser-Add-on: Backup WhatsApp Chats
  - Export als HTML oder CSV inkl. Bilder und Videos

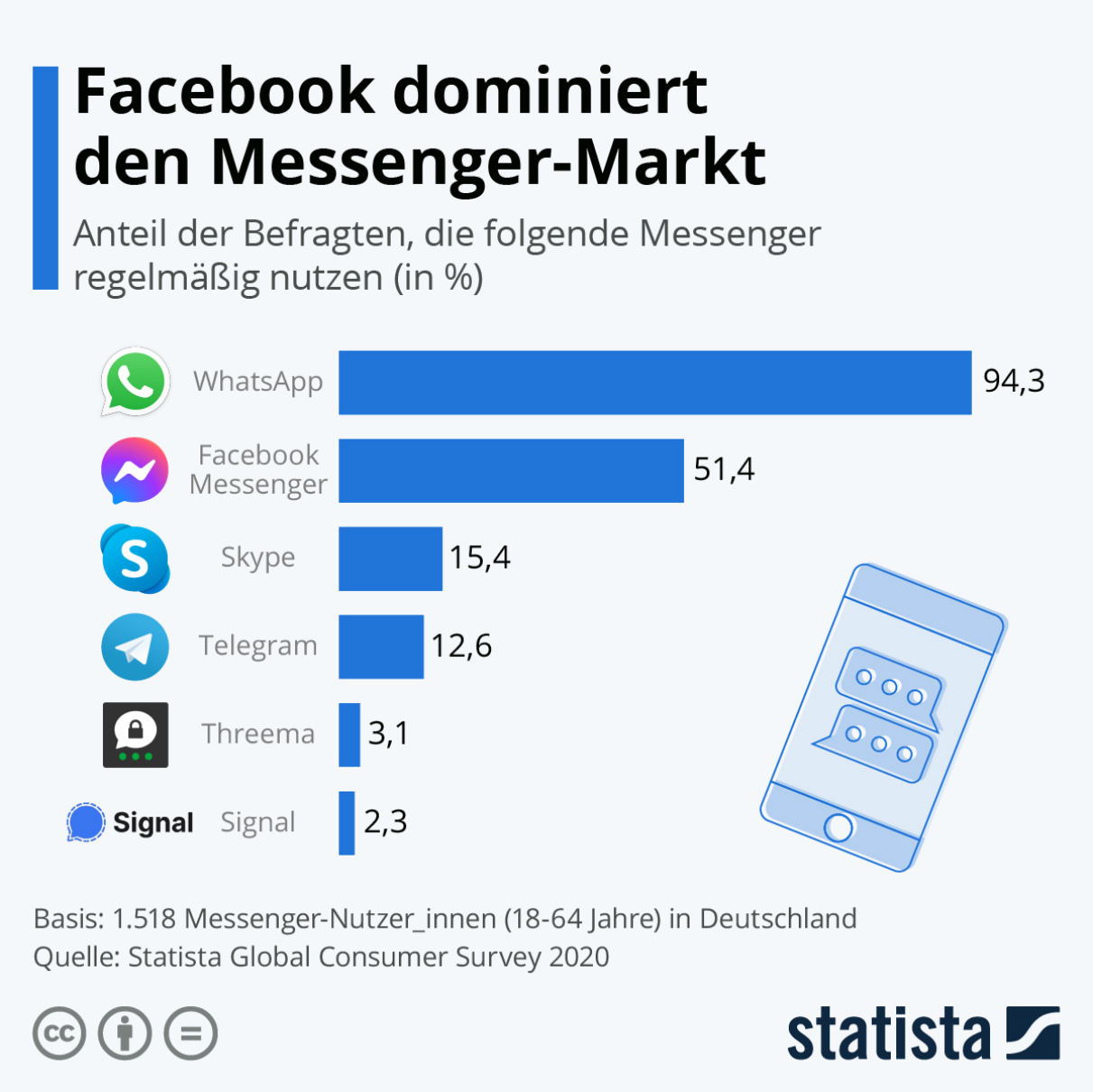
2. Teil
Bitte nicht vom Regen in die Traufe

www.flaticon.com / CC 3.0 BY

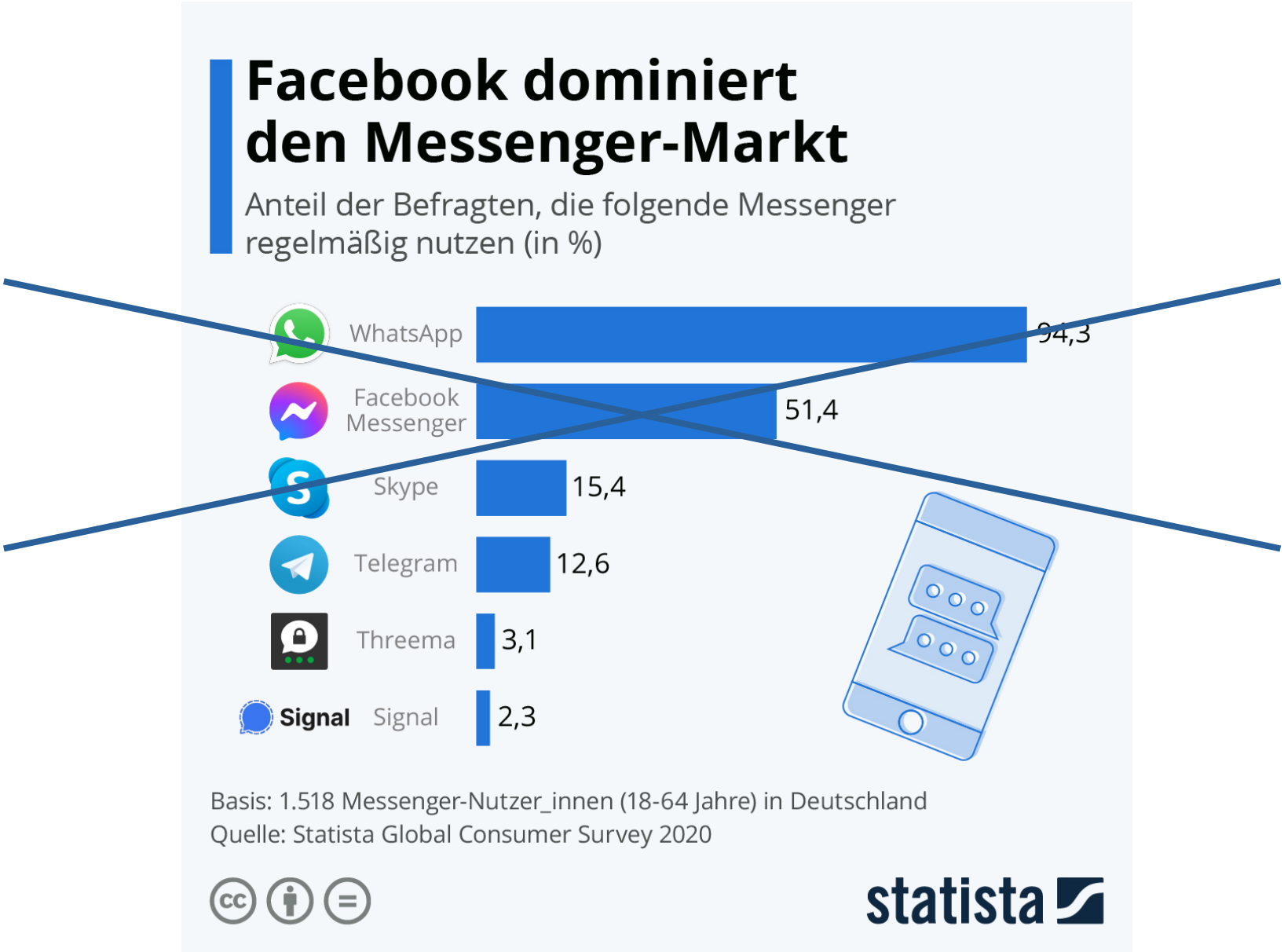
www.flaticon.com / CC 3.0 BY

Tschüss WhatsApp! Aber wohin?

- Es gibt gute Gründe sich von WhatsApp/Facebook zu verabschieden
- Aber wohin soll man wechseln?
- Stand 27.04.2021 Wikipedia gibt es aktuell ca. 30 bekannte Messenger
- Davon sind vielleicht eine Handvoll empfehlenswert



Von: statista
Quelle: https://de.statista.com/infografik/23449/umfrage-zur-nutzung-von-messengern-in-deutschland/



Von: statista
Quelle: https://de.statista.com/infografik/23449/umfrage-zur-nutzung-von-messengern-in-deutschland/

Fokus auf Sicherheit und Datenschutz

- Der »ideale« Messenger aus Sicherheits- bzw. Datenschutzperspektive:
  - Freie und quelloffene Software (FOSS)
  - Vermeidung der Erfassung/Verarbeitung von Metadaten
  - Vorzugsweise föderierte Infrastruktur oder P2P-Kommunikation
  - Kryptografie – bewährte Verfahren, kein eigenes »Gebastel«
    - Ende-zu-Ende-Verschlüsselung (E2EE)
    - Folgenlosigkeit (Perfect Forward Secrecy)
    - Authentifizierungsmöglichkeit Kontakte
  - Keine integrierten Tracker, die Nutzer »ausspionieren«
  - Frei wählbarer Identifier (nicht zwingend Telefonnummer)
  - Bestätigung der Sicherheit durch unabhängige Audits

Telegram

Open-Source	●
FOSS	●
Metadaten	●
Föderiert/P2P	●
Kryptografie	●
Identifier	●

✓ Multi-Client-fähig

✗ Keine Angaben zum Umgang mit Metadaten

Standardmäßig nicht E2E-verschlüsselt

In Gruppenchats gar keine E2EE

Nachrichten für Betreiber lesbar

Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

	Telegram	Threema
Open-Source	🟡	🟡
FOSS	🟡	🟠
Metadaten	🟠	🟡
Föderiert/P2P	🟠	🟠
Kryptografie	🟡	🟢
Identifier	🟡	🟢

Telegram

✓ Multi-Client-fähig

✗ Keine Angaben zum Umgang mit Metadaten

Standardmäßig nicht E2E-verschlüsselt

In Gruppenchats gar keine E2EE

Nachrichten für Betreiber lesbar

Threema

✓ Ohne Verknüpfung einer Telefonnummer nutzbar

Standardmäßig E2E-verschlüsselt

Oftmals (unabhängig) auditiert

✗ Serverpart nicht quelloffen

Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

	Telegram	Threema	Signal
Open-Source	🟡	🟡	🟢
FOSS	🟡	🟠	🟠
Metadaten	🟠	🟡	🟢
Föderiert/P2P	🟠	🟠	🟠
Kryptografie	🟡	🟢	🟢
Identifier	🟡	🟢	🟡

Telegram

✓ Multi-Client-fähig

✗ Keine Angaben zum Umgang mit Metadaten

Standardmäßig nicht E2E-verschlüsselt

In Gruppenchats gar keine E2EE

Nachrichten für Betreiber lesbar

Threema

✓ Ohne Verknüpfung einer Telefonnummer nutzbar

Standardmäßig E2E-verschlüsselt

Oftmals (unabhängig) auditiert

✗ Serverpart nicht quelloffen

Signal

✓ Setzt Maßstäbe (Signal-Protokoll, Sealed-Sender)

Standardmäßig E2E-verschlüsselt

Kein zentraler Messenger vermeidet Metadaten besser

✗ Telefonnummer notwendig

Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

	Telegram	Threema	Signal	Conversations (XMPP)
Open-Source	🟡	🟡	🟢	🟢
FOSS	🟡	🟠	🟠	🟢
Metadaten	🟠	🟡	🟢	🟠
Föderiert/P2P	🟠	🟠	🟠	🟢
Kryptografie	🟡	🟢	🟢	🟢
Identifier	🟡	🟢	🟡	🟢
✓	Multi-Client-fähig	Ohne Verknüpfung einer Telefonnummer nutzbar Standardmäßig E2E-verschlüsselt Oftmals (unabhängig) auditiert	Setzt Maßstäbe (Signal-Protokoll, Sealed-Sender) Standardmäßig E2E-verschlüsselt Kein zentraler Messenger vermeidet Metadaten besser	Muli-Client-fähig Standardmäßig E2E-verschlüsselt Ohne Verknüpfung einer Telefonnummer nutzbar
✗	Keine Angaben zum Umgang mit Metadaten Standardmäßig nicht E2E-verschlüsselt In Gruppenchats gar keine E2EE Nachrichten für Betreiber lesbar	Serverpart nicht quelloffen	Telefonnummer notwendig	XMPP-Unterbau nicht für die Vermeidung von Metadaten konzipiert

Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Kein Walled-Garden

	Telegram	Threema	Signal	Conversations (XMPP)	Element (Matrix)
Open-Source	🟡	🟡	🟢	🟢	🟢
FOSS	🟡	🟠	🟠	🟢	🟢
Metadaten	🟠	🟡	🟢	🟠	🟠
Föderiert/P2P	🟠	🟠	🟠	🟢	🟢
Kryptografie	🟡	🟢	🟢	🟢	🟢
Identifier	🟡	🟢	🟡	🟢	🟢

Telegram

✓ Multi-Client-fähig

✗ Keine Angaben zum Umgang mit Metadaten

Standardmäßig nicht E2E-verschlüsselt

In Gruppenchats gar keine E2EE

Nachrichten für Betreiber lesbar

Threema

✓ Ohne Verknüpfung einer Telefonnummer nutzbar

Standardmäßig E2E-verschlüsselt

Oftmals (unabhängig) auditiert

✗ Serverpart nicht quelloffen

Signal

✓ Setzt Maßstäbe (Signal-Protokoll, Sealed-Sender)

Standardmäßig E2E-verschlüsselt

Kein zentraler Messenger vermeidet Metadaten besser

✗ Telefonnummer notwendig

Conversations (XMPP)

✓ Muli-Client-fähig

Standardmäßig E2E-verschlüsselt

Ohne Verknüpfung einer Telefonnummer nutzbar

✗ XMPP-Unterbau nicht für die Vermeidung von Metadaten konzipiert

Element (Matrix)

✓ Muli-Client-fähig

Standardmäßig E2E-verschlüsselt

Ohne Verknüpfung einer Telefonnummer nutzbar

✗ Matrix-Protokoll nicht für die Vermeidung von Metadaten konzipiert

3. Teil

Messenger: Zielgruppe und eigene Anforderungen/Bedürfnisse sind (mit-)entscheidend

www.flaticon.com / CC 3.0 BY

Geeignet je nach Zielgruppe

- Zusätzlich zu den technischen Kriterien sollte bei der Wahl unbedingt auch berücksichtigt werden:
  - Zielgruppe
  - Benutzerfreundlichkeit (steht in Beziehung zur Zielgruppe)
  - Eigene (individuelle) Anforderungen/Bedürfnisse

Geeignet je nach Zielgruppe

- Zusätzlich zu den technischen Kriterien sollte bei der Wahl unbedingt auch berücksichtigt werden:
  - Zielgruppe
  - Benutzerfreundlichkeit (steht in Beziehung zur Zielgruppe)
  - Eigene (individuelle) Anforderungen/Bedürfnisse

Durchschnittsnutzer
Benutzerfreundlichkeit: **Hoch**

Geeignet für WhatsApp-Wechselwillige

Ähnlicher Komfort bzw. Bedienbarkeit

Wenig Metadaten und sicher

Threema | Signal

Geeignet je nach Zielgruppe

- Zusätzlich zu den technischen Kriterien sollte bei der Wahl unbedingt auch berücksichtigt werden:
  - Zielgruppe
  - Benutzerfreundlichkeit (steht in Beziehung zur Zielgruppe)
  - Eigene (individuelle) Anforderungen/Bedürfnisse

Durchschnittsnutzer
Benutzerfreundlichkeit: **Hoch**

Geeignet für WhatsApp-Wechselwillige

Ähnlicher Komfort bzw. Bedienbarkeit

Wenig Metadaten und sicher

Threema | Signal

Fortgeschrittene
Benutzerfreundlichkeit: **Mittel**

Für Nutzer mit hohem Autonomiebedürfnis

Freie Serverwahl bzw. keine Bindung an Anbieter

Conversations | Element
(XMPP | Matrix)

Geeignet je nach Zielgruppe

- Zusätzlich zu den technischen Kriterien sollte bei der Wahl unbedingt auch berücksichtigt werden:
  - Zielgruppe
  - Benutzerfreundlichkeit (steht in Beziehung zur Zielgruppe)
  - Eigene (individuelle) Anforderungen/Bedürfnisse

Durchschnittsnutzer
Benutzerfreundlichkeit: **Hoch**

Geeignet für WhatsApp-Wechselwillige

Ähnlicher Komfort bzw. Bedienbarkeit

Wenig Metadaten und sicher

Threema | Signal

Fortgeschrittene
Benutzerfreundlichkeit: **Mittel**

Für Nutzer mit hohem Autonomiebedürfnis

Freie Serverwahl bzw. keine Bindung an Anbieter

Conversations | Element (XMPP | Matrix)

Journalisten/Aktivisten
Benutzerfreundlichkeit: **Niedrig**

Dezentrale, zensurresistene Kommunikation

Verschleierung von Metadaten und sicher

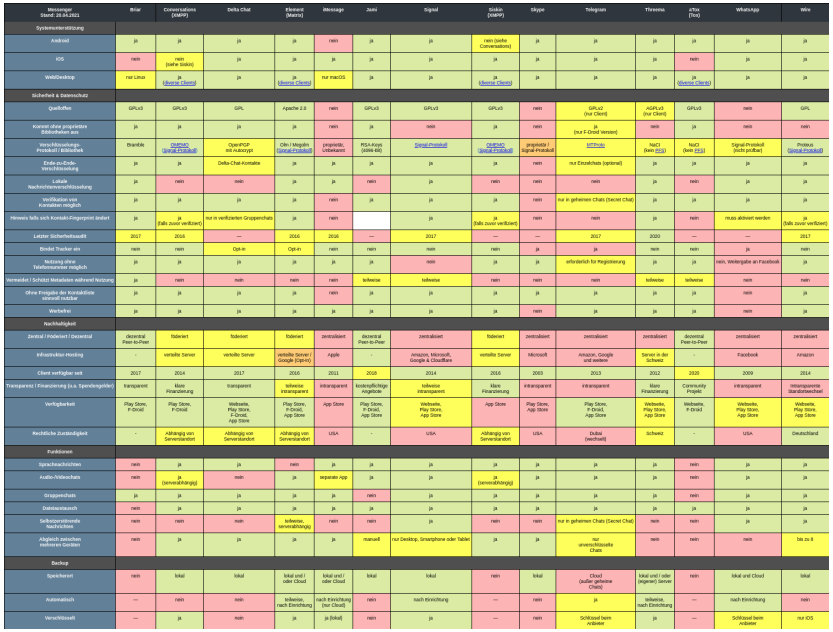
Briar (nur Android)

Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Messenger-Matrix

- Vergleicht 14 Messenger
- Überblick über 30 verschiedene Merkmale
- www.messenger-matrix.de (Deutsch/Englisch)

Messenger Stand: 20.04.2021	Signal	Telegram	Threema	WhatsApp
Sicherheit & Datenschutz				
Quelloffen	GPLv3	GPLv2 (nur Client)	AGPLv3 (nur Client)	nein
Kommt ohne proprietäre Bibliotheken aus	nein	ja (nur F-Droid Version)	nein	nein
Verschlüsselungs-Protokoll / Bibliothek	Signal-Protokoll	MTProto	NaCl (kein PFS)	Signal-Protokoll (nicht prüfbar)
Ende-zu-Ende-Verschlüsselung	ja	nur Einzelchats (optional)	ja	ja
Lokale Nachrichtenverschlüsselung	ja	nein	ja	ja
Verifikation von Kontakten möglich	ja	nur in geheimen Chats (Secret Chat)	ja	ja



Fazit

- Datenschutzfreundliche WhatsApp-Alternativen sind vorhanden
- Orientieren Sie sich bei einem Wechsel an...
  - ... den vorgestellten Messengern
  - ... an der Zielgruppe
  - und ihren eigenen (individuellen) Anforderungen

Familie, Freunde, und Bekannte mitnehmen

- Nicht drängen / missionieren
- Parallelbetrieb möglich
- Gemeinsam ausprobieren
- Aufzeigen, was Alternativen besser machen

Viel Geduld ...

Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Vielen Dank …

- … für Ihre Aufmerksamkeit!
- … für Ihre Fragen!

Mike Kuketz
Dipl.-Inform. (FH)

Tel.: +49 (0) 711 / 615541-65
Mail: kuketz@lfdi.bwl.de

Bildquellen [1]

- Jungle
  Autor: Freepik
  Lizenz: www.flaticon.com / CC 3.0 BY
- Lightning
  Autor: Freepik
  Lizenz: www.flaticon.com / CC 3.0 BY
- Rain
  Autor: Freepik
  Lizenz: www.flaticon.com / CC 3.0 BY
- Wave
  Autor: iconixar
  Lizenz: www.flaticon.com / CC 3.0 BY
- Confrontation
  Autor: Freepik
  Lizenz: www.flaticon.com / CC 3.0 BY