Stand der Technik nach DSGVO am Beispiel Kopano - Was sagt ChatGPT?

> Auf Nachfrage interessierte mich die Meinung von ChatGPT zum Thema Übergangsfristen für abgelaufene Software, wie z. B. Kopano u. Ä. Nicht immer schafft man rechtzeitig die Migration auf aktuelle Systeme, meist wegen der Absprachen und Termin- und Kostengespräche mit Kunden

Nach der Datenschutz-Grundverordnung (DSGVO) gibt es **keine ausdrücklichen Übergangsfristen** für die Pflicht, Serversoftware auf dem *Stand der Technik* zu halten. Die Verordnung trat am 25. Mai 2018 in Kraft und gilt seither unmittelbar in allen EU-Mitgliedstaaten.

Was bedeutet "Stand der Technik" laut DSGVO?

Die DSGVO verlangt in **Art. 32 Abs. 1** von Verantwortlichen und Auftragsverarbeitern geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dabei ist **„der Stand der Technik“** ein zentrales Kriterium.

Das bedeutet konkret:

- Sicherheitslücken in Server- oder Anwendungssoftware **müssen zeitnah** geschlossen werden.
- Der Einsatz **nicht mehr unterstützter oder veralteter Software** (z. B. alte PHP-Versionen, Windows 7, EOL-Linux-Distributionen) ist **nicht zulässig**, wenn dadurch Sicherheitsrisiken entstehen.

Gibt es trotzdem Spielräume oder Fristen?

Zwar gibt es **keine festen Fristen in der DSGVO**, aber:

- In der Praxis **kann** bei Updates oder Umstellungen ein **kurzer Zeitraum** zur Umsetzung toleriert werden – **solange ein Risikoanalyse- und Migrationsplan dokumentiert ist**.
- Bei Audits oder Vorfällen ist entscheidend, ob du als Verantwortlicher:
  - Risiken erkannt hast,
  - Maßnahmen geplant und priorisiert hast,
  - dokumentieren kannst, warum du etwas wie schnell umgesetzt hast.

Beispiele:

Software	Stand der Technik?	Kommentar
Ubuntu 20.04	Ja (bis 2025)	Unterstützt, wenn regelmäßig aktualisiert
Windows Server 2012 R2	Nein (EOL)	Nicht mehr sicher, nicht DSGVO-konform
Apache 2.2	Nein	Veraltet, seit Jahren nicht mehr unterstützt
Nextcloud (aktuelle LTS-Version)	Ja	Regelmäßige Updates, DSGVO-konform

Fazit:

- **Keine Übergangsfristen** – aber Planung und dokumentierte Risikobewertung sind wichtig.
- Veraltete Software = hohes Bußgeldrisiko bei Datenschutzverstößen.
- IT-Sicherheitsrichtlinien (z. B. vom BSI oder ISO 27001) helfen bei der Definition des „Stands der Technik“.

Wenn du willst, kann ich dir eine Checkliste zur DSGVO-konformen Server-Softwarepflege erstellen.

> Das Problem mit **Kopano Groupware unter Univention Corporate Server (UCS) 5.0** liegt **mittelfristig vor allem beim Thema "Stand der Technik"** im Sinne der DSGVO – insbesondere in Bezug auf:

□□ 1. **Veraltete Softwarebasis von Kopano**

- **Kopano Core** (insbesondere `kopano-server`, `kopano-webapp`, `kopano-spooler` usw.) wird **seit längerer Zeit kaum weiterentwickelt**.
- Sicherheits- und Bugfix-Updates erscheinen **selten oder gar nicht mehr regelmäßig**.
- Einige Komponenten (z. B. `kopano-webmeetings`, `kopano-dagent`, `kopano-z-push`) sind teilweise **nicht mehr kompatibel mit aktuellen PHP-Versionen**, was ein Sicherheitsrisiko darstellt.

➡ **Risiko**: Wenn Sicherheitslücken bekannt werden und keine Updates folgen, ist der „Stand der Technik“ **nicht mehr gegeben**.

□□ 2. **Eingeschränkte oder fehlende Wartung im UCS App Center**

- Kopano war lange im UCS App Center verfügbar, wurde aber teilweise **nicht mehr aktiv gepflegt**.
- Mit der Umstellung auf UCS 5.0 wurden viele Altpakete nicht migriert oder sind nur mit manuellem Aufwand nutzbar.
- **Kopano4UCS**, ein Community-Projekt, hat zwar Lösungen bereitgestellt, diese gelten **nicht als offizieller Supportpfad**.

➡ **Risiko**: Kein garantierter Support, keine klare Roadmap, und Integration in UCS nur noch teilweise gepflegt.

□□ 3. **Unklare Sicherheitsgarantie & Datenschutzfolgeabschätzung**

- Nach DSGVO musst du jederzeit **nachweisen können**, dass deine Systeme sicher sind.
- Bei Kopano ist eine fundierte **Datenschutzfolgeabschätzung (DSFA)** kaum möglich, wenn:
  - keine Sicherheitsupdates veröffentlicht werden,
  - unklar ist, wie Daten verschlüsselt übertragen oder gespeichert werden,

- keine aktuellen Dokumentationen verfügbar sind.

➡ **Risiko**: Du trägst die volle Haftung bei Datenpannen – auch wenn die Ursache eine nicht gewartete Drittsoftware ist.

4. **Abhängigkeit von veralteten Komponenten**

- PHP, MariaDB/MySQL, Apache-Versionen, auf die Kopano setzt, sind oft nicht mehr im Mainstream-Support.
- Anpassungen an moderne Umgebungen (z. B. systemd, PHP 8.2+, OpenLDAP unter UCS 5.0) erfolgen **nicht zuverlässig**.

➡ **Risiko**: Du bleibst auf alten Softwareständen – was DSGVO-widrig ist.

Fazit: Wo ist mittelfristig das Problem?

Bereich	Risiko	DSGVO-Auswirkung
Sicherheitspatches fehlen	Hoch	Kein „Stand der Technik“
Keine Updates über App Center	Mittel	Wartung erschwert
Keine klare Produkt-Roadmap	Hoch	Planbarkeit & DSFA unmöglich
Technische Abhängigkeiten	Mittel bis hoch	Zunehmende Inkompatibilität

Empfehlung

Wenn du Kopano (noch) nutzt:

- Erstelle eine **Risikoanalyse** und dokumentiere die Abhängigkeit.
- Plane **mittelfristig die Migration** (z. B. auf Open-Xchange, EGroupware, Nextcloud Groupware + Mailcow).
- Prüfe Alternativen mit aktivem Hersteller-Support und Sicherheitszertifizierungen.

Wenn du möchtest, kann ich dir eine **Migrations-Checkliste** oder Alternativen zu Kopano unter UCS zusammenstellen.

Version #2
Erstellt: 2025-06-30 10:53:37 UTC von Christian Zengel (sysops GmbH)
Zuletzt aktualisiert: 2025-06-30 10:58:08 UTC von Christian Zengel (sysops GmbH)