

IT-sikkerhed for advokatkontorer

GDPR, fortrolighed og Schrems II i praksis

— en 12-siders håndbog til danske advokatvirksomheder

I DENNE GUIDE

- Advokatsamfundets krav til IT, fortrolighed og klientdata
- GDPR artikel 32 & 9 — hvad det betyder for jeres kontor
- Schrems II & US Cloud Act for Microsoft 365 og Google Workspace
- Praktisk 10-trins sikkerhedsbaseline + leverandør-tjekliste
- Beredskab og kommunikation ved databrud — første 24 timer

Forfatter

Michael Wolf — stifter, IT-Hjælpen ApS

10+ års erfaring med IT-drift, sikkerhed og GDPR for SMV

Version 1.0 · May 2026 · it-hjaelpen.com/ressourcer

Indhold

1. Introduktion: Hvorfor advokatkontorer er et særligt mål	3
2. Det juridiske fundament — GDPR, RPL og Advokatsamfundet	4
3. Schrems II og US Cloud Act i en advokatkontekst	5
4. Risikobillede 2026 — de fem hyppigste trusler	6
5. 10-trins sikkerhedsbaseline for advokatkontorer	7
6. Cloud-valg: Microsoft 365, Google Workspace eller EU-stak?	8
7. Leverandør-tjekliste — databehandleraftaler i praksis	9
8. Beredskab — de første 24 timer efter et databrud	10
9. Awareness — træning af partnere, advokater og sekretærer	11
10. Næste skridt og om IT-Hjælpen	12

Sådan bruger du guiden

Læs kapitel 1-3 som ledelses-overblik. Brug kapitel 5 og 7 som arbejdsdokumenter — print dem, sæt initialer på, og gem dem som dokumentation til Datatilsynet. Tjeklisterne i kapitel 5, 7 og 8 er bevidst korte nok til at kunne gennemføres på en eftermiddag.

1. Introduktion: Hvorfor advokatkontorer er et særligt mål

Advokatkontorer behandler nogle af de mest værdifulde data, der findes i dansk erhvervsliv: M&A-aftaler under forhandling, retssager med konkurrerende parter, persondata i kategori-9 (sundhed, strafbare forhold, fagforening), og fortrolige klientstrategier. For en angriber er et mellemstort advokatkontor en kort vej til informationer, der kan kursmanipuleres, sælges videre eller bruges som afpresningsmateriale.

Det er ikke en hypotetisk risiko. De seneste år har bl.a. Bech-Bruun, britiske Ince & Co og amerikanske Mossack Fonseca alle været ramt af alvorlige IT-hændelser med konkrete konsekvenser for klienter, omdømme og licensforhold. For et dansk SMV-advokatkontor (5-30 ansatte) er det realistiske risikobillede dog ikke statsstøttede angreb, men **ransomware, phishing og fejlhåndteret cloud-konfiguration** — og det er præcis dér, denne guide har fokus.

Hvad guiden gør — og hvad den ikke gør

- **Gør:** giver en praktisk, dansk-baseret baseline I kan implementere på 4-6 uger.
- **Gør:** oversætter Schrems II, Cloud Act og GDPR til konkrete handlinger.
- **Gør ikke:** erstatter en formel risikovurdering eller en DPO.
- **Gør ikke:** tager stilling til de specifikke advokatetiske spørgsmål — det hører Advokatsamfundet til.

Hovedpointe

Advokatkontorer falder ofte mellem to stole: store nok til at have alvorlige compliance-krav, men sjældent store nok til at have en intern IT-chef eller DPO. Det er præcis den situation, en ekstern IT-partner skal aflaste.

2. Det juridiske fundament

GDPR artikel 5, 9 og 32

GDPR artikel 5(1)(f) kræver, at persondata behandles med **integritet og fortrolighed**. Artikel 32 konkretiserer dette til foranstaltninger som kryptering, adgangskontrol, testning og hændeshåndtering. For advokater er artikel 9 særligt vigtig: data om strafbare forhold, fagforening, sundhed og seksuelle forhold må kun behandles på et afgrænset lovgrundlag og kræver *skærpede* sikkerhedsforanstaltninger.

Retsplejeloven og tavshedspligten

Retsplejeloven § 129 og straffelovens § 152 fastslår advokaters tavshedspligt. Den gælder uændret, selv når data ligger i Microsoft 365, Google Drive eller en privat e-mailkonto. Datatilsynet har gentagne gange understreget, at en advokat **ikke kan delegere ansvaret bort** ved at bruge en cloud-leverandør — ansvaret for konfiguration, adgangsstyring og valg af leverandør forbliver hos advokaten som dataansvarlig.

Advokatsamfundets vejledning

Advokatrådet har siden 2018 anbefalet, at advokatkontorer gennemfører en formel risikovurdering af deres IT-miljø og dokumenterer både tekniske og organisatoriske foranstaltninger. Manglende dokumentation er én af de hyppigste anker ved tilsyn — ikke selve hændelsen, men det at man ikke kan vise, at man har gjort sig overvejelserne.

Konkret krav

Som minimum skal jeres kontor kunne fremvise: (1) artikel 30-fortegnelse, (2) databehandleraftaler med alle leverandører, (3) risikovurdering, (4) procedure for håndtering af brud, og (5) dokumentation af tekniske foranstaltninger.

3. Schrems II og US Cloud Act

EU-Domstolens Schrems II-dom (2020) erklærede USA's *Privacy Shield* ugyldig. Konsekvensen: overførsel af persondata til USA — eller til amerikansk-ejede cloud-tjenester — kræver en konkret risikovurdering (TIA, Transfer Impact Assessment) og typisk supplerende tekniske foranstaltninger som kryptering, hvor kun I har nøglen.

Hvad er US Cloud Act?

CLOUD Act (2018) giver amerikanske myndigheder ret til at kræve data fra amerikanske cloud-leverandører, uanset hvor i verden data fysisk er hostet. Det betyder, at selv hvis jeres Microsoft 365-data ligger i et datacenter i Dublin, kan FBI eller en amerikansk domstol kræve dem udleveret — og leverandøren må ifølge amerikansk ret som udgangspunkt ikke informere jer om det.

Hvorfor er det særligt for advokater?

For en advokat er fortrolighed ikke valgfri. Hvis I behandler en sag mod et amerikansk selskab, eller en klient med interesser i USA, kan ren brug af M365/Google Workspace udgøre et reelt fortroligheds- og habilitetsproblem — uanset hvad GDPR siger. Datatilsynet har i 2022-2024 udtrykkeligt anbefalet EU-baserede alternativer for kategori-9-data og for sektorer med skærpet fortrolighed.

Tre realistiske spor

1) Bliv på M365/Google + lav TIA, BYOK-kryptering og adgangsstyring. **2)** Hybrid: M365 til standard kontorarbejde, EU-stak (Nextcloud + Mailbox.org) til klientmapper og kategori-9-data. **3)** Fuld EU-stak — typisk for kontorer med store offentlige klienter eller skærpet fortrolighed.

4. Risikobillede 2026

Baseret på Center for Cybersikkerheds trusselsvurdering, Datatilsynets afgørelser og IT-Hjælpens egne sager hos danske advokatkontorer er dette de fem hyppigste trusler.

Område	Risiko	Konsekvens	Anbefaling
Phishing & BEC	Høj	Falske fakturaer, klientidentitetstyveri, MFA-angreb, aflevering af klientmateriale	Phishing-sikring, MFA, DMARC + DKIM + SPF + DMARC p=reject + årlig awareness
Ransomware	Høj	Krypterede sagsmapper, dage uden adgang til data	Tidlig oplysning til politiet (90 dage), EDR, segmenteret netværk, backup
Cloud-fejlkonf.	Middel	Klientdata delt offentligt via SharePoint	Standard for data-deling = OFF, DLP-regler, kvartalsvis review
Insider/exit	Middel	Tidligere ansat tager sagsmateriale med	Off-boardering, tjek af adgang, USB-restriktion, OneDrive-hold
Schrems II / Cloud Act	Middel	GDPR-bøde, klientklage, advokatetisk klage	Tjek af BYOK eller EU-stak for kategori-9 og sager mod US-parter

Bemærk

Phishing er stadig den hyppigste indgang. 90+ % af alle hændelser hos danske SMV'er starter med en e-mail. Den enkleste investering med størst effekt er fortsat MFA + et avanceret mailfilter — i den rækkefølge.

5. 10-trins sikkerhedsbaseline

Dette er den minimumsbaseline, IT-Hjælpen anbefaler for danske advokatkontorer med 5-30 ansatte. Print siden, sæt initialer ud for hvert punkt, og opbevar den som dokumentation til Datatilsynet og Advokatsamfundet.

1. MFA på alle konti — også admin og delegerede postkasser Conditional Access kræver MFA for 100 % af brugerne. Ingen undtagelser, heller ikke for partnere.
2. Password-manager + politik mod genbrug 1Password Business eller Bitwarden Teams. Bloker svage/genbrugte kodeord.
3. Centralt administreret EDR på alle endpoints Microsoft Defender for Business, SentinelOne eller Bitdefender GravityZone.
4. Automatisk patching af OS og Microsoft 365 Apps Intune eller RMM. SLA: kritiske patches inden 7 dage.
5. Tredjeparts backup af M365 / Google Workspace Min. 90 dages opbevaring, immutable, testet gendannelse hvert halve år.
6. Avanceret phishing-filter + DMARC p=reject Defender for Office Plan 1 + SPF, DKIM, DMARC med rua-rapportering.
7. Adgangsstyring efter mindste-privilegium-princippet Sagsmapper deles per-sag, ikke per-bruger. Kvartalsvis review af adgange.
8. Off-boarding-procedure ved fratrædelse Konto deaktiveres samme dag, postkasse holdes 90 dage, data eksporteres til arkiv.
9. Skriftlig IT- og brudprocedure (1-2 sider) Hvem isolerer, hvem ringer til hvem, hvor ligger backup-nøglerne.
10. Årlig awareness-træning + simuleret phishing 30 min. e-learning + 4 phishing-simuleringer pr. år. Dokumentér deltagelse.

6. Cloud-valg: M365, Google eller EU-stak?

Der findes ikke ét rigtigt svar. Valget afhænger af klientportefølje, sagstyper og kontorets tolerance for kompleksitet. Tabellen nedenfor sammenligner de tre realistiske spor for et dansk advokatkontor med 5-30 ansatte.

	Microsoft 365	Google Workspace	EU-stak (Nextcloud + Mailbox.org)
Funktionalitet	Mest komplet, Word/Excel natursk	Stærk samarbejde, svagere Of	Off
Schrems II-risiko	Middel-høj (US-ejet)	Middel-høj (US-ejet)	Lav (EU-ejet, EU-hostet)
Pris (10 brugere/md.)	~2.500-3.500 kr.	~1.500-2.500 kr.	~1.000-1.800 kr.
Integration med dansk ret	Består af mest udbredt)	OK	Kræver tilpasning
Egnet til kategori-9-data	Kun med BYOK + TIA	Kun med BYOK + TIA	Ja, uden supplerende foranstaltninger
Anbefales til	Kontorer med standardklienter	Kontorer der lever i Google i fo	Kontorer med offentlige klienter eller skærpet fortrolighed

Pragmatisk anbefaling

For de fleste danske advokatkontorer er en **hybrid model** det rette valg: M365 til kalender, mail og dagligt kontorarbejde + Nextcloud (hostet i EU) til klientmapper med følsomme data. Det giver kompatibilitet med resten af branchen og minimerer Schrems II-eksponeringen på de data, der virkelig betyder noget.

7. Leverandør-tjekliste — DPA i praksis

GDPR artikel 28 kræver, at I har en databehandlersaftale (DPA) med **alle** leverandører, der behandler persondata på jeres vegne. Det gælder også 'små' tjenester: e-signatur, regnskab, CRM, kalender-add-ons. Brug tjeklisten nedenfor til hver leverandør.

DPA underskrevet og opbevaret Skriftlig aftale, dateret, opbevaret centralt (ikke kun i e-mail).
Underdatabehandlere er listet og godkendt Krav om varsel ved ændringer. Tjek listen mindst én gang om året.
Hostingland er angivet EU/EØS = ok. Tredjelande kræver TIA og supplerende foranstaltninger.
Sletteprocedure ved kontraktophør Skriftligt bekræftet — typisk 30-90 dage efter opsigelse.
Brudnotificering inden 24 timer Leverandøren skal kunne notificere jer hurtigt nok til at I kan overholde 72-timersfristen.
Sikkerhedscertificering (ISO 27001 eller tilsvarende) Anmod om kopi af seneste audit-rapport eller SOC 2 Type II.
Cyberforsikring eller ansvarsdækning Spørg ind til leverandørens forsikringsdækning ved sikkerhedshændelser.
Eksportmulighed af jeres data I skal kunne få jeres data ud i et almindeligt format (CSV, JSON, PST).

Praktisk tip

Lav en simpel Excel-fortegnelse med kolonner: *leverandør*, *formål*, *datakategorier*, *hostingland*, *DPA dato*, *sidste review*. Det er typisk nok til at tilfredsstille både artikel 30 og en Datatilsynsforespørgsel.

8. Beredskab — første 24 timer efter et databrud

GDPR giver jer **72 timer** til at notificere Datatilsynet efter konstatering af et brud. I praksis afgøres jeres tab i de første 4 timer. Brug denne sekvens som skabelon til jeres egen 1-siders beredskabsplan.

0-30 min	Identificér og isolér Tag berørte enheder offline, men sluk dem ikke (bevar hukommelse til efterforskning). Ring til IT-partner.
30-90 min	Skab overblik Hvilke konti, sagsmapper og klienter er berørt? Aktiver beredskabsgruppen (partner, IT, evt. ekstern jurist).
2-4 timer	Begræns og kommunikér internt Skift kodeord på berørte konti, revoker sessions, informer ansatte om hvad de må sige (og ikke sige).
4-12 timer	Forberede notificering Vurder om kriterierne i artikel 33 er opfyldt. Dokumentér tidslinje og foranstaltninger.
12-24 timer	Notificér Datatilsynet hvis krævet Brug Datatilsynets online formular. Notificér også berørte klienter hvis det er nødvendigt jf. artikel 34.
24+ timer	Efterforskning og lessons learned Gem logs, lav rapport til Advokatsamfundet hvis relevant, opdater beredskabsplan.

Hvem ringer du til?

Skriv det ned *før* det sker: IT-partner, cyberforsikring, evt. ekstern DPO, Datatilsynet (33 19 32 00), Advokatsamfundet. Print listen og hæng den op fysisk — ransomware kan også låse jeres egen kontaktbog.

9. Awareness — træning af partnere og medarbejdere

Teknik stopper de fleste angreb, men ikke alle. Den sidste 10 % afhænger af, om en advokat klikker på et link i en falsk faktura fra en "klient". Awareness handler ikke om at gøre folk paranoide, men om at give dem nok genkendelse til at stoppe og spørge.

Et realistisk årshjul

	Q1 — Onboarding-modul (30 min) Alle nye ansatte gennemfører grundmodul om phishing, kodeord, GDPR-basics.
	Q1 — Simuleret phishing #1 Bred kampagne mod alle. Dokumentér klikrate som baseline.
	Q2 — Live workshop (60 min) Partnermøde med eksempler på faktiske angreb mod danske advokatkontorer.
	Q2 — Simuleret phishing #2 Målrettet kampagne med advokat-specifikke scenarier (CC af modpart, falsk klientkonto).
	Q3 — Mikro-læring (5 min) Korte videoklip om aktuelle trusler — kvartalsmail med 1-2 tips.
	Q3 — Simuleret phishing #3 BEC-scenari: 'partner' beder sekretær om hasteoverførsel.
	Q4 — Tabletop-øvelse (90 min) Beredskabsgruppen simulerer et ransomware-scenari uden teknik — kun procedurer.
	Q4 — Simuleret phishing #4 + rapport Mål forbedring fra Q1. Dokumentér til ledelsen og evt. cyberforsikring.

Dokumentation

Gem deltagerlister og resultater. Det er ofte den dokumentation, der gør forskellen på en bødeforhøjelse og en bødenedsættelse hos Datatilsynet, hvis det værste sker.

10. Næste skridt

Hvis I har læst hertil og kan svare "ja" til alle 10 punkter i kapitel 5, er I bedre stillet end ca. 80 % af danske advokatkontorer. Hvis ikke, er den hurtigste vej fremad typisk:

- **Uge 1:** Tag vores gratis sikkerheds-tjek — få et baseline-tal og en PDF-rapport.
- **Uge 2:** Implementér MFA på alle konti og aktivér avanceret phishing-filter.
- **Uge 3-4:** Tilkøb tredjeparts backup og test gendannelse af én postkasse + én sagsmappe.
- **Uge 5-6:** Opdatér jeres artikel 30-fortegnelse og indsaml manglende DPA'er.
- **Løbende:** Sæt awareness-årshjulet i gang og book årlig review med IT-partner.

Vil I have hjælp?

IT-Hjælpen fungerer som ekstern IT-afdeling for danske advokatkontorer. Vi tager ansvar for drift, sikkerhed, M365-administration og GDPR-dokumentation — på en fast månedlig pris uden binding ud over almindelig opsigelse.

Book en gratis 30-minutters IT-gennemgang: it-hjaelpen.com/kontakt · 60 19 12 13 · kontakt@it-hjaelpen.com

Om forfatteren

Michael Wolf er stifter af IT-Hjælpen ApS og har 10+ års erfaring med IT-drift, sikkerhed og GDPR for danske SMV'er — herunder en række advokatkontorer på Sjælland og i Hovedstaden. Michael har baggrund i Microsoft 365-administration og har bygget IT-Hjælpen som specifikt SMV-fokuseret alternativ til de store IT-huse.

Denne guide er en generel vejledning og erstatter ikke konkret juridisk eller IT-faglig rådgivning. © IT-Hjælpen ApS 2026. Må frit deles i sin helhed med kildehenvisning.