KAILA

(kommune)

Compliance Whitepaper

Version 1.0
September 2025

KARNOV GROUP

Indholdsfortegnelse

1. Resumé

KAILA er en AI-assistent implementeret af Karnov Group Denmark A/S (Karnov Group), der understøtter juridisk vejledning, videns søgning og compliance i kommunerne og for andre fagfolk.

Løsningen kombinerer adgang til det juridiske indhold i Karnov Groups database og organisationens egne retningslinjer med fokus på informationssikkerhed, brugervenlighed, digital tilgængelighed og overholdelse af gældende regler og standarder. KAILA er ikke trænet i hverken Karnov Groups indhold eller de interne retningslinjer fra den relevante organisation, men baserer sine svar på indholdet.

Alle brugere har adgang til KAILA og kan stille spørgsmål i applikationen via tekstindtastning. Organisationens egne retningslinjer kan kun uploades af relevante medarbejdere inden for organisationen.

Dette whitepaper beskriver vores forpligtelse til datasikkerhed, privatlivets fred og overholdelse af EU-reglerne med hensyn til KAILA.

2. Brug af data i KAILA

2.1 Databehandlingsroller i KAILA

Karnov Group fungerer som dataansvarlig for personoplysninger, der indsamles i forbindelse med levering og administration af vores licenserede produkter og vores tjenester – herunder aktiviteter såsom kontoadministration, fakturering, kundesupport og analyser relateret til generel produktanvendelse (f.eks. søgeforespørgsler og serviceinteraktionslogfiler).

Som dataansvarlig fastlægger Karnov Group formålet med og midlerne til behandling af brugsdata, som kan analyseres med henblik på produktforbedring, sikkerhedsovervågning, overholdelse og statistiske formål, altid i overensstemmelse med gældende lovgivning om databeskyttelse.

Licenshaveren er dog en uafhængig dataansvarlig for de indtastninger, som brugeren foretager i KAILA, og det er derfor den enkelte brugers ansvar at sikre, at hverken følsomme forretningsoplysninger eller personoplysninger behandles i strid med gældende lovgivning. Yderligere oplysninger findes i Karnov Groups **generelle licensbetingelser**.

2.2 Hvilke data indsamles og lagres i KAILA?

Bruger-id, adgangslogdata, brugerinput og uploadede interne retningslinjer gemmes kun for at understøtte brugerens arbejde. Personoplysninger bør ikke uploades eller behandles. Data i KAILA, herunder brugerens input, bruges udelukkende til at give brugeren et svar. Kun hvis brugeren giver feedback på svarene, vil dette blive brugt til at forbedre KAILA. Hvis en brugers input og/eller output skal bruges til at forbedre KAILA, vil det blive anonymiseret inden brug og adskilt fra den enkelte bruger.

En brugers input gemmes i KAILA og forbliver tilgængeligt for brugeren i 90 dage siden sidste aktivitet i den specifikke samtale, medmindre det er fastgjort, i hvilket tilfælde det gemmes, indtil brugeren sletter det eller fjerner fastgørelsen. Dette giver brugeren mulighed for at genbesøge tidligere input eller stille yderligere spørgsmål om det samme emne. Fastgjorte samtaler opbevares, indtil de enten slettes aktivt af brugeren eller indtil kundeaftalen ophører.

2.3 Upload og brug af interne dokumenter

KAILA er ikke beregnet til at modtage eller behandle personoplysninger. Brugere bør ikke indtaste eller uploade personoplysninger. Karnov Group behandler kun tekniske oplysninger (f.eks. bruger-id, adgangslogfiler) med henblik på sikker drift, adgangsstyring og overholdelse af regler. Ingen

data behandles eller opbevares uden for EU/EØS.

KAILA giver organisationen mulighed for at uploade sine egne interne retningslinjer, politikker og procedurer. Disse dokumenter er tilgængelige for brugeren via løsningen og understøtter konsistens, kvalitet og vidensdeling. Uploadede dokumenter er kun til organisationens interne brug.

2.4 Hvor opbevares KAILAs data?

KAILA er en cloudbaseret SaaS-løsning, hvilket betyder, at data ikke er fysisk placeret hos Karnov Group. Karnov Group bruger i øjeblikket Google Cloud Platform i Tyskland og Holland samt Microsoft Azure Cloud Platform og tjenester i Holland, Irland og Sverige. Data behandles derfor ikke uden for EU/EØS. Fysisk adgang til servere er begrænset til autoriseret personale hos Google og Microsoft.

2.5 Hvem har adgang til data i KAILA?

Alle medarbejdere hos Karnov Group med brugerrettigheder i KAILA bliver sikkerhedstjekket og godkendt, før de får adgang til vores udviklings- og driftsmiljøer. Tekniske roller, der er ansvarlige for support og vedligeholdelse af KAILA, kan få adgang til data for at undersøge fejl og ydeevneproblemer. Vores udviklingsteam kan få adgang til anonyme søgedata for at optimere modeladfærd, udvælgelse og ydeevne.

Karnov Group har implementeret klare rolle og adgangsstyringsprocedurer, og al privilegeret adgang til hele platformen kræver multifaktor-autentificering på bruger-, enheds- og netværksniveau.

Kundernes brugere eller administratorer kan til enhver tid slette deres egne indtastninger og dokumenter, hvorefter sletningen er permanent.

2.6 Hvad bruges KAILA-data til?

Data i KAILA, herunder brugerens input, bruges udelukkende til at give brugeren et svar. Kun hvis brugeren giver feedback på KAILAs svar, vil dette blive brugt til at forbedre KAILA. Hvis en brugers input og/eller KAILAs output skal bruges til at forbedre KAILA, vil det blive anonymiseret før brug og adskilt fra den enkelte bruger. Se også afsnit 8 om opbevaring og sletning af data nedenfor.

3. Brugeradministration og integration

3.1 Central brugeradministration

Afhængigt af abonnementstypen kan adgang til det licenserede produkt gives på en af følgende måder:

- **Adgang via Microsoft Entra ID (Azure AD)**: Brugeradgang administreres via kundens Microsoft Entra ID, hvilket muliggør centraliseret oprettelse, de-aktivering og tilladelsesadministration i overensstemmelse med kundens egne identitetsstyringspolitikker. Denne metode muliggør sikkert login med multifaktor-autentificering, anvendelse af

adgangskodepolitikker og adgangslogning i overensstemmelse med kundens sikkerhedsindstillinger. Ændringer i brugers adgang træder i kraft med det samme, og der er ingen integration med andre kundesystemer ud over Entra ID. Læs mere om, hvordan brugeradministration fungerer: Karnov Kundeportal Dokumentation

- **Adgang via personlig adgangskode**: Kun brugere, der har fået udstedt en personlig adgangskode af Karnov Group i henhold til kundeaftalen med licenstageren, er autoriseret til at bruge det licenserede produkt. Hver bruger kan logge ind fra maksimalt tre enheder samtidigt. Licenshaveren og dens brugere må ikke give tredjeparter adgang til det licenserede produkt via online-tjenester, internettet, intranettet eller på anden måde, og må heller ikke dele de adgangskoder, der er udstedt af Karnov Group, med tredjeparter. Hvis licenshaveren er en virksomhed, offentlig eller privat institution, organisation osv., må den ikke give adgang til andre medarbejdere end dem, der har fået udstedt en personlig adgangskode.

- **Adgang via IP-adresse**: Licenstageren må kun få adgang til det licenserede produkt fra den IP-adresse og de fysiske placeringer, der er angivet i ordrebekræftelsen. En aftale, der giver adgang via licenstagerens IP-adresse, kan under visse betingelser give licenstagerens medarbejdere mulighed for at anmode om en personlig adgangskode til de erhvervede produkter. En personlig adgangskode forbliver aktiv indtil aftalens ophør, medmindre den pågældende medarbejders ansættelse hos licenstageren ophører tidligere. Licenshaveren er ansvarlig for at underrette Karnov Group om enhver ophørt ansættelse, da retten til at bruge den personlige adgangskode ophører straks fra ophørsdatoen.

4 Organisatoriske kontroller

4.1 Rammer for datastyring

Governance-strukturer definerer og fordeler sikkerhedsansvaret på tværs af organisationen. Politikker udarbejdes, godkendes af ledelsen og gennemgås regelmæssigt for at sikre effektiviteten.

Der er udpeget en CISO for koncernen, og et informationssikkerhedsudvalg overvåger overholdelsen og risikostyringen.

Karnov Group opretholder en **tre-linjers** forsvarsmodel for at styre cyber- og informationssikkerhed effektivt.

1. Første linje: Forretningsenheder og drift (herunder IT-driftssikkerhed og produktudvikling)

2. Anden linje: Cybersikkerhed og compliancefunktion

3. Tredje linje: Intern revision og virksomhedsrisikostyring (ERM)

Hver linje har forskellige ansvarsområder, hvilket sikrer, at governance og risikostyring både er

integreret i driften og sikres uafhængigt.

4.2 Tredjepartsstyring

Leverandører kategoriseres efter den sikkerhedsrisiko, deres tjenester udgør for Karnov Group. Alle leverandører med middel og høj risiko skal udfylde et spørgeskema om informationssikkerhed og bestå den sikkerhedsvurdering, der foretages af Karnov Groups sikkerhedspersonale. Karnov Group gennemgår årligt højrisikoleverandørers overholdelse af reglerne, og leverandørers sikkerhedshændelser spores, og deres indvirkning på Karnov Groups informationer og tjenester vurderes løbende.

4.3 Overholdelsesrevision

Karnov Group har et dedikeret team, der overvåger og implementerer ændringer i lovgivningen og overvåger relevant lovgivning for at sikre streng overholdelse af al relevant lovgivning i vores jurisdiktion.

5 Personale kontroller

5.1 Adgangsstyring

Der er indført rollebaseret adgangskontrol for at sikre, at kun autoriseret personale har adgang til følsomme systemer og data. Tilladelser er baseret på mekanismer for mindst mulig adgang og forretningsmæssige behov, og der foretages regelmæssige gennemgange for at opretholde passende adgangsniveauer.

5.2 Uddannelse og awareness

Security awareness er et centralt element i Karnov Groups sikkerhedsstrategi. Alt personale skal gennemføre årlig uddannelse inden for alle relevante compliance-områder, såsom informationssikkerhed, privatliv, kunstig intelligens osv.

Der gennemføres flere phishing-simuleringstests om året, og de erfaringer, der gøres, anvendes i kvartalsvise security awareness kampagner med fokus på nye trusler og bedste praksis.

6 Fysiske kontroller

6.1 Kontorsikkerhed

Aktive medarbejdere har adgang til Karnov Groups kontorlokaler via et adgangskort. Det er let at skelne mellem medarbejdere, konsulenter og besøgende ved hjælp af forskellige farver på kortindehavernes kort. Kontorerne er beskyttet med alarmsystemer, der er forbundet med fysiske sikkerhedsleverandører, der er tilgængelige 24/7 for at reagere på enhver alarmaktivering.

6.2 Cloududbyders sikkerhed

Cloud-løsninger fra Google (Google Cloud Platform) og Microsoft (Microsoft Azure) bruges til hosting af de licenserede produkter, der er udviklet af Karnov Group. Den understøttende

infrastruktur er fysisk placeret i europæiske datacentre i Tyskland, Holland og Irland. Fysisk adgang til serverne er begrænset til autoriseret personale fra Google og Microsoft.

7 Teknologiske kontroller

7.1 Dataminimering og privatliv

Karnov Group anvender forbedrede dataminimeringsteknikker ved at sikre, at kun nødvendige data bruges til at generere svaret til brugeren.

7.2 Håndtering af tekniske sårbarheder

Karnov Group har implementeret automatiseret patch-styring, sikkerhedsscanning og årlige penetrationstest.

8 Datasikkerhed og privatliv

8.1 Kryptering og adgangskontrol

Al kommunikation mellem klient og server og mellem servere i KAILA er krypteret, hvilket sikrer, at netværkstrafikken ikke kan opfanges af tredjeparter.

Alle samtaler – herunder alle brugerinput og genererede output – krypteres in transit og at rest.

8.2 Dataisolering

KAILA bruger logisk dataisolering for at sikre, at brugerdata er adskilt og ikke kan tilgås af andre brugere. Brugerinput bruges aldrig til modeltræning eller -forbedring uden fuldstændig forudgående anonymisering.

8.3 Retsgrundlag for behandling af personoplysninger

Karnov Group behandler de data, der genereres ved brug af de licenserede produkter, på grundlag af legitime interesser, jf. artikel 6, stk. 1, litra f), i den generelle forordning om databeskyttelse. Oplysningerne bruges til at levere de licenserede produkter, til markedsføring, til at forbedre it-sikkerhed, til kommunikation og til udvikling af de licenserede produkter.

8.4 Den registreredes rettigheder

Som registreret har man en række rettigheder, som man kan udøve ved at kontakte os på **privacy@karnovgroup.com** eller ved at sende os et brev. Læs mere om dine rettigheder i vores **privatlivspolitik**.

8.5 Behandling af personoplysninger af tredjeparter:

Karnov Group benytter tredjepartsleverandører til at levere hosting, infrastruktur og relaterede tjenester, der er nødvendige for driften af KAILA. Leverandører kategoriseres efter den sikkerhedsrisiko, deres tjenester udgør for Karnov Group. Alle leverandører med middel og høj risiko skal

udfylde et spørgeskema om informationssikkerhed og bestå en sikkerhedsvurdering, der udføres af Karnov Groups sikkerhedsteam.

Når Karnov Group fungerer som uafhængig dataansvarlig, kan tredjeparter behandle begrænsede personoplysninger, der er nødvendige for at levere platformen og sikre dens sikre drift.

Microsoft – Microsoft Azure Cloud Platform og tjenester, hostet i datacentre inden for EU/EØS (Holland, Irland, Sverige).

Google – Google Cloud Platform og tjenester, hostet i datacentre inden for EU/EØS (Tyskland, Holland).

Derudover bruger KAILA **Azure OpenAI** (via Microsoft Azure) og **Google Vertex AI** (via Google Cloud Platform) til AI-drevet behandling for at generere svar baseret på Karnov Groups juridiske indhold og brugerinput. Vi forbeholder os ret til at ændre eller opdatere de specifikke store sprogmodeller (LLM'er), der bruges, forudsat at enhver udskiftning er inden for disse udbyderes nuværende serviceudbud og hostes under de samme EU/EØS-dataplaceringskontroller.

9 Opbevaring og sletning af data

9.1 Opbevaringspolitikker

For at give brugerne mulighed for at vende tilbage til en tidligere interaktion og fortsætte deres arbejde gemmes samtaler – herunder alle brugerinput, genererede output og eventuelle uploadede dokumenter – for den enkelte bruger.

Alle samtaler **slettes automatisk 90 dage efter den seneste aktivitet** i den pågældende samtale, medmindre samtalen er markeret som *fastgjort* af brugeren, i hvilket tilfælde opbevaringen følger de fastgørelsesregler, der er fastsat i kundens aftale.

Hvis en bruger sletter en samtale manuelt, slettes hele samtalen – inklusive alle uploadede dokumenter og alle relaterede output – permanent og irreversibelt.

10 Tilgængelighed (digital tilgængelighed)

KAILA er udviklet med fuld fokus på digital tilgængelighed for alle brugere. Løsningen vedligeholdes og udvikles i overensstemmelse med WCAG-standarder, hvilket sikrer, at indhold og funktioner er:

- **Opfattelige:** Information og brugergrænseflade kan opfattes af alle brugere, f.eks. gennem klar kontrast, alternativ tekst og tekst-til-tale-indstillinger.
- **Betjenelige:** Alle interaktioner og navigation kan udføres via tastatur og skærmlæsere.
- **Forståelige:** Kommunikation og funktioner er klare og intuitive, så alle sagsbehandlere kan udnytte platformen fuldt ud.

- **Robust:** Indholdet kan fortolkes af en lang række enheder og hjælpemidler og understøtter fremtidige standarder.

Tilgængeligheden overvåges løbende, og forbedringer dokumenteres i Karnov Groups udviklingslog. Dokumentation om tilgængelighed og testresultater er tilgængelige på anmodning.

11 Browserkompatibilitet

KAILA understøtter alle større, opdaterede browsere (2 år gamle eller nyere) på både stationære og mobile enheder, men løsningen er ikke specifikt optimeret til mobil brug. For en komplet oversigt over understøttede browsere, besøg vores **side om browserkompatibilitet.**

Der kræves internetforbindelse for at kunne bruge løsningen.

12 AI-etik og -styring

Karnov Group strukturerer AI-governance og -kontrol omkring de syv etiske principper, der er fastsat i præamblen til EU's AI-Act, gennem en model for risikostyring og en risikobaseret tilgang.

KAILA er et beslutningsstøtteværktøj under menneskelig kontrol og betragtes ikke som et højrisiko-AI-system i henhold til AI-Acts nuværende anvendelsesområde.

AI-Act er i øjeblikket kun trådt i kraft for forbudte AI-systemer og modeller til generelle formål, som falder uden for anvendelsesområdet for KAILA. Desuden regulerer AI-Act primært højrisiko-AI-systemer, som defineret i artikel 6 og bilag III, og KAILA falder **ikke** ind under disse kategorier, da det ikke bruges til beslutninger, der har en væsentlig indvirkning på individers grundlæggende rettigheder, sundhed eller sikkerhed.

12.1 Menneskelig indgriben og tilsyn

KAILA er designet som et hjælpemiddel, der understøtter, **men ikke** erstatter, menneskelig beslutningstagning. Det er underlagt menneskelig kontrol og tilsyn og træffer ikke automatiske beslutninger, der har væsentlig indflydelse på enkeltpersoners grundlæggende rettigheder, sundhed eller sikkerhed. Brugerne informeres via grænsefladen og brugsbetingelserne om, at det kun skal bruges som et hjælpemiddel og ikke kan erstatte professionel juridisk rådgivning.

Karnov Group har udviklet et AI-forklaringsmodul, der giver brugerne indsigt i KAILAs proces og funktionalitet.

12.2 Teknisk robusthed og sikkerhed

KAILAs tekniske robusthed og sikkerhed sikres gennem vores modelrisikostyringsramme, som er i overensstemmelse med EU's AI-Act.

Hver ændring af kodebasen eller de underliggende store sprogmodeller evalueres ved hjælp af en kombination af automatiserede interne benchmarks og ekspertvurderinger foretaget af domænespecialister for at verificere ydeevnen og mindske fejl.

Platformen gennemgår regelmæssige sikkerhedstests, herunder automatiseret patch-styring, kontinuerlig sikkerhedsscanning og årlige penetrationstests udført af certificerede fagfolk, for hurtigt at opdage og afhjælpe sårbarheder.

For at opretholde pålideligheden og aktualiteten af det juridiske indhold opdateres de underliggende juridiske informationskilder ugentligt og frigives først til produktion, når test og kvalitetskontrol er bestået, hvilket hjælper med at forhindre forringelse og utilsigtede effekter i downstream-svar.

Sammen styrker disse kontroller modstandsdygtigheden over for misbrug eller ændringer, der kan påvirke ydeevnen, og reducerer risikoen for utilsigtet skade på brugere og tredjeparter.

12.3 Privatliv og datastyring

KAILA opretholder privatliv og stærk datastyring gennem dataminimering, sikkerhedskontrol ved design og klar livscyklusstyring. Kun de data, der er nødvendige for at generere et svar, behandles, og al kommunikation mellem klient og server og mellem servere krypteres under overførslen.

Af hensyn til kontinuiteten opbevares brugerinput og genererede output for den enkelte bruger, i **90 (halvfems)** dage eller indtil brugeren sletter dem. Når en samtale slettes, fjernes den fuldstændigt og irreversibelt.

Behandlingen af brugsgenererede data er baseret på legitime interesser i henhold til artikel 6, stk. 1, litra f i GDPR, og de registrerede kan udøve deres rettigheder ved at kontakte privacy@karnov-group.com.

KAILA er ikke beregnet til at behandle personoplysninger, så tredjepartsbehandling af persondata er ikke påkrævet; hvis omfanget ændres til at inkludere upload af personoplysninger, vil det juridiske grundlag blive opdateret tilsvarende.

12.4 Gennemsigtighed

KAILA er designet til at være gennemsigtig med hensyn til sine muligheder, begrænsninger og drift. Et AI-forklaringsmodul og en ledsagende vejledning giver indsigt i, hvordan svarene genereres, og muliggør informeret brugerovervågning.

12.5 Mangfoldighed, ikke-diskrimination og retfærdighed

KAILA fungerer som et værktøj til beslutnings under menneskelig overvågning for og bidrager til at

reducere risikoen for diskriminerende automatiserede resultater. Modelkvaliteten vurderes løbende ved hjælp af automatiserede interne benchmarks, der suppleres med ekspertvurderinger for at identificere problemer og mindske uberettigede fordomme.

Dataminimering og logisk adskillelse af brugerdata reducerer yderligere eksponeringen for unødvendige attributter. Disse foranstaltninger understøtter samlet set en retfærdig og ligelig anvendelse i forskellige sagsbehandlingssammenhænge, samtidig med at mennesker bevarer kontrollen over de endelige beslutninger.

12.6 Samfundsmæssig og miljømæssig velfærd

KAILA er udviklet og drives i overensstemmelse med Karnov Groups ESG-strategi. Karnov Group er forpligtet til at følge koncernens mission om at bane vejen for retfærdighed, der er knyttet til fem af FN's verdensmål, især verdensmål 16, fred, retfærdighed og stærke institutioner.

Vi er forpligtet til at minimere miljøpåvirkningen ved at reducere drivhusgasemissioner og materialebehov i overensstemmelse med gældende miljølovgivning og med løbende forbedringer gennem mål og overvågning.

Vi respekterer og opretholder internationalt anerkendte menneskerettigheder, fremmer et sikkert, inkluderende og sundt arbejdsmiljø og inddrager interessenter og leverandører for at fremme ansvarlig praksis og sikre, at vores værdikæde overholder tilsvarende ESG-standarder. ESG-governance sikres gennem bestyrelsens tilsyn, etisk adfærd, integration af ESG-risikostyring i vores ERM-proces, gennemsigtig rapportering og ansvarlighedsmekanismer, herunder vores adfærdskodeks og whistleblower-politik.

12.7 Ansvarlighed

Ansvarlighed for KAILA er forankret i Karnov Groups AI- og dataetikpolitik og Karnov Groups AI-instruktion sammen med en model for risikostyring, der er i overensstemmelse med EU's AI-Act. Klare tekniske og organisatoriske kontroller – herunder centraliseret adgangsstyring, intern back-end-adgang, detaljeret login-logning, regelmæssige sikkerhedstests og penetrationstests samt krypteret kommunikation – fastlægger ansvar og revisionsmuligheder på tværs af tjenesten. Karnov Group forpligter sig til at underrette kunderne uden unødig forsinkelse om ethvert brud på persondata og præciserer i sine licensbetingelser, at KAILA er et hjælpemiddel og ikke erstatter professionel juridisk rådgivning, hvilket styrker klare roller og ansvarsområder over for brugere og berørte personer.

13. Overholdelse og ansvar

13.1 Underretning om brud på datasikkerheden

Karnov Group vil uden unødig forsinkelse underrette kunden i tilfælde af brud på databeskyttelsen vedrørende kundens bruger.

13.2 Ansvar og erstatning

Karnov Groups licensbetingelser angiver udtrykkeligt, at KAILA er et hjælpemiddel og ikke erstatter professionel juridisk rådgivning.

14. Revisionslog

Version	Gældende fra	Revisionskategori Ny/Opdatering/Formulering/Ingen	Beskrivelse af vigtigste revisioner
1.0	01.09.2025	Ny	Første version til kunder i den offentlige sektor

Kontakt: **privacy@karnovgroup.com**