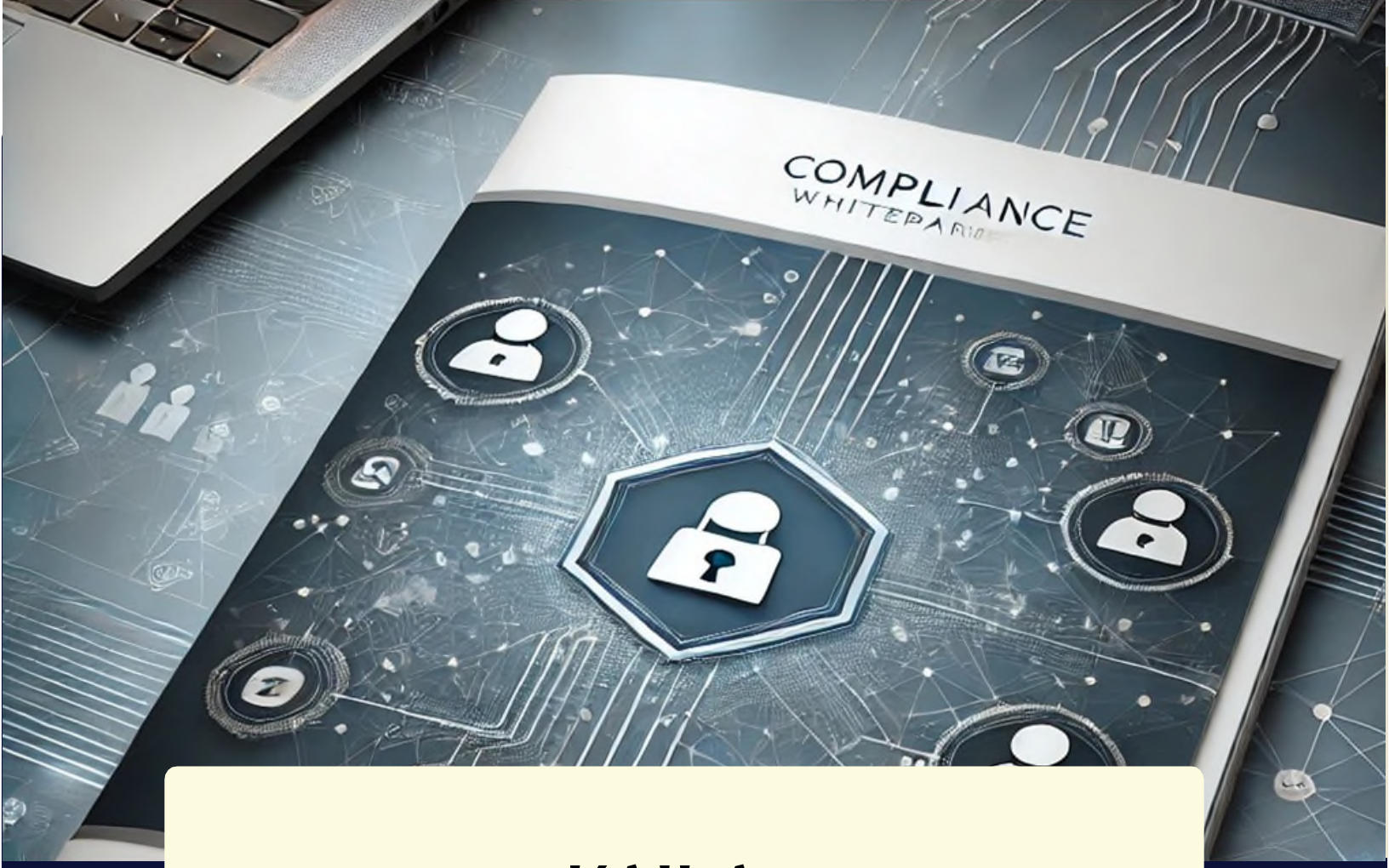


# KAILA

## (jura)

# Compliance whitepaper

**Version 3.0**

**September 2025**

KARNOV GROUP

# Indholdsfortegnelse

# 1. Sammenfatning

KAILA[1] er en AI-assistent implementeret af Karnov Group Denmark A/S (Karnov Group) til at søge i sin database med juridisk indhold og give svar på kundeforespørgsler. KAILA er **ikke** trænet i Karnov Groups indhold, men baserer sine svar på indholdet. Alle brugere har adgang til chatten og kan stille spørgsmål i applikationen via tekstindtastning.

Ud over sine kernefunktioner indeholder KAILA en dokumentanalysefunktion, der giver brugerne mulighed for at uploade dokumenter til AI-assisteret juridisk gennemgang. Denne funktion tilbyder fire forskellige analysemuligheder: Styrk argumenter, find svagheder, complianceanalyse og kontraktanalyse. Hver funktion er udviklet i samarbejde med erfarne jurister og AI-specialister. Ud over disse foruddefinerede analyser har brugerne også mulighed for at uploade dokumenter direkte i deres samtale med KAILA. Dette giver brugeren mulighed for at tilføje præcis kontekst og lade KAILA analysere materialet – for eksempel ikke-offentliggjort retspraksis fra kundens arkiver.

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

[1] KAILA (jura)

# 2. Brug af data i KAILA

## 2.1. Dataansvarlig og databehandlers ansvar for vores licenserede produkter

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. søgninger og logs over interaktioner med vores tjenester).

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

For alle data, som brugeren indtaster i KAILA (herunder input og uploadede dokumenter), er Kunden dog dataansvarlig. Karnov Group behandler udelukkende disse data på vegne af Kunden og fungerer som databehandler som defineret i GDPR. Databehandlingen i KAILA er reguleret af en databehandleraftale [DBA] baseret på Datatilsynets standardkontraktbestemmelser, som er en integreret del af kundeaftalen. Det er kundens ansvar at sikre, at der er et gyldigt retsgrundlag for behandlingen af data i KAILA, og at al behandling overholder gældende lovgivning.

For yderligere information henvises til Karnov Groups til enhver tid gældende licensvilkår.

## 2.2 Hvilke data indsamles og lagres i KAILA?

KAILA indsamler og gemmer begrænsede data for at understøtte brugerens arbejde og leveringen af tjenesten.

- **Når** Karnov Group **fungerer som selvstændig dataansvarlig** (f.eks. brugeradgang, kundesupport osv.), gemmer Karnov Group **bruger-id og adgangslogdata i relation til KAILA.**
- **Når** Karnov Group **fungerer som databehandler** i relation til behandlingsaktiviteter inden for KAILA, **gemmer virksomheden både samtaleinput og alt uploadet indhold**. Typen og arten af uploadet indhold bestemmes udelukkende af Kunden, som er Dataansvarlig. **Al sådan behandling udføres i overensstemmelse med kundens instrukser som defineret i databehandleraftalen (DPA).**

I forhold til slettepolitik for opbevaring ad data henvises til dette whitepapers afsnit 9.

Oplysninger, der indtastes i chatten i KAILA, bruges udelukkende til at generere et svar til brugeren. De tilgås eller behandles ikke til andre formål, medmindre brugeren vælger at give feedback på et givet svar. I sådanne tilfælde kan de relevante data – både brugerens input og KAILAs output – tilgås af Karnov Group udelukkende med det formål at forbedre KAILA. Det er vigtigt at

bemærke, at disse data altid vil blive anonymiseret og adskilt fra bruger-id'et, før de bruges til udvikling eller kvalitetsforbedring.

### 2.3 Hvor opbevares KAILAs data?

KAILA er en cloudbaseret SaaS-løsning, hvilket betyder, at data ikke opbevares på Karnov Groups egne lokationer. I stedet bruger Karnov Group Google Cloud Platform i Tyskland og Holland samt Microsoft Azure Cloud Platform og tjenester i Holland, Irland og Sverige. Som følge heraf behandles alle data udelukkende inden for EU/EØS.

### 2.4 Hvem har adgang til data i KAILA?

Alle medarbejdere med brugerrettigheder i KAILA gennemgår en grundig sikkerhedskontrol, inden de får adgang til vores udviklings- og driftsmiljøer. Tekniske medarbejdere, der er ansvarlige for support og vedligeholdelse af KAILA, kan få adgang til data, hvis det er nødvendigt for at undersøge fejl og ydeevneproblemer. Vores data analytikere har kun adgang til anonymiserede data for at optimere KAILAs svar, udvælgelse og ydeevne.

Karnov Group har implementeret klare procedurer og kontroller for rolle- og adgangsstyring. Al privilegeret adgang til platformen kræver multifaktor-autentificering på bruger-, enheds- og netværksniveau.

### 2.5 Hvad bruges KAILA-data til?

Data i KAILA, herunder brugerinput, bruges udelukkende til at generere et svar til brugeren. For eksempel behandles et uploadet dokument udelukkende med henblik på at udføre den valgte analyse (f.eks. kontraktgennemgang, compliance-gennemgang), hvilket betyder, at resultater og udtrukne data udelukkende bruges i forbindelse med den pågældende samtale og ikke bruges til at træne modeller.

## 3. Brugeradministration og integration

Afhængigt af omfanget i Kundeaftalen gives adgang til det eller de relevante licenserede produkter enten via kundens IP-adresse, via individuelle brugeres personlige konti eller en kombination af begge dele.

Kunden og dens bruger(e) må ikke give tredjeparter adgang til de licenserede produkter og må heller ikke videregive loginoplysninger udstedt af licensgiveren til tredjeparter. En bruger kan logge ind via personlige konti til de licenserede produkter fra højst tre (3) enheder ad gangen. Kunden og dens bruger(e) må ikke videregive de udstedte adgangskoder.

- **Adgang via personlige brugerkonti:** En personlig adgangskode forbliver aktiv indtil kundekontraktens ophør, medmindre den pågældende medarbejders ansættelse hos kunden ophører tidligere. Kunden er ansvarlig for at underrette Karnov Group om enhver ophørt ansættelse, da retten til at bruge den personlige adgangskode ophører straks fra ansættelsens ophørsdato.

    - **Microsoft Entra ID (Azure AD)**: Brugeradgang administreres via kundens Microsoft Entra ID, hvilket muliggør centraliseret oprettelse, de-aktivering og administration af tilladelser i overensstemmelse med kundens egne identitetsstyringspolitikker. Denne metode muliggør sikkert login med multifaktor-godkendelse, anvendelse af adgangskodepolitikker og adgangslogning i overensstemmelse med kundens sikkerhedsindstillinger. Ændringer i brugeradgang træder i kraft med det samme, og der er ingen integration med andre kundesystemer ud over Entra ID. Læs mere om, hvordan brugeradministration fungerer her: Karnov Kundeportal Dokumentation (På engelsk)

    - **Adgang via personlige legitimationsoplysninger genereret af Karnov Group**: Brugeradgang administreres og vedligeholdes af Karnov Group, og de brugere, som Karnov Group har udstedt personlige legitimationsoplysninger til, kan bruge dem til at logge ind på de licenserede produkter.

- **Adgang via IP-adresse**: Kunden kan få adgang til det licenserede produkt fra de IP-adresser, der er aftalt i forbindelse med indgåelsen af Kundeaftalen. Adgang via kundens IP-adresse kan under visse betingelser give kundens medarbejdere mulighed for at anmode om en personlig adgangskode til de erhvervede produkter.

# 4. Organisatoriske kontroller

## 4.1 Rammeværk for datastyring

Karnov Group har implementeret en governance-struktur, der definerer og fordeler sikkerhedsansvaret på tværs af organisationen. Der er udviklet politikker, som godkendes af ledelsen og regelmæssigt gennemgås for at sikre effektiviteten.

Der er udpeget en Group CISO, og et informationssikkerhedsudvalg overvåger compliance og risikostyring.

Karnov Group opretholder en tre-linjers forsvarsmodel for at administrere 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 risikostyring (Enterprise Risk Management – ERM)

Hver linje har forskellige ansvarsområder, hvilket sikrer, at governance og risikostyring både er integreret i driften og sikres uafhængigt.

### 4.2 Styring af tredjeparter

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 sikkerhedshændelser hos leverandører overvåges, og deres indvirkning på Karnov Groups information, produkter og tjenester vurderes løbende.

### 4.3 Compliance tilsyn

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 rollebaserede adgangskontrolforanstaltninger for at sikre, at kun autoriseret personale har adgang til følsomme systemer og data. Tilladelser tildeles i henhold til **princippet om mindst mulig adgang** og **forretningsbehov**, og der foretages regelmæssige gennemgange for at sikre, at de relevante adgangsniveauer opretholdes.

### 5.2 Uddannelse og awareness

Security awareness er en central del af Karnov Groups sikkerhedsstrategi**. Alt personale skal gennemføre en årlig uddannelse inden for alle relevante compliance-områder,** herunder informationssikkerhed, privatliv og kunstig intelligens.

Der gennemføres phishing-simuleringstests flere gange om året, og de erfaringer, der gøres, anvendes til løbende forbedringer. Derudover afholdes der kvartalsvise security awareness kampagner for at adressere nye trusler og fremme best practice.

# 6. Fysiske kontroller

## 6.1 Kontorsikkerhed

Aktive medarbejdere har adgang til Karnov Groups lokaler 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 til et alarmselskab, der er tilgængelige 24/7 for at reagere på enhver aktivering ad en alarm.

## 6.2 Cloududbyderes 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, Sverige og Irland. Fysisk adgang til serverne er begrænset til autoriseret personale fra Google og Microsoft.

# 7. Teknologiske kontroller i KAILA

## 7.1 Dataminimering og privatliv

Karnov Group anvender optimerede 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, genererede output og alle uploadede dokumenter – krypteres in transit og at rest ved hjælp af en brugerspecifik krypteringsnøgle. Disse krypteringsnøgler opbevares separat og er **kun** tilgængelige **for autoriseret teknisk personale** med et arbejdsrelateret behov, efter strenge procedurer for adgangstilladelse.

### 8.2 Dataisolering

KAILA bruger logisk dataisolering for at sikre, at brugerdata er adskilt og ikke kan tilgås af andre brugere.

### 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 GDPR. Oplysningerne bruges til at levere vores licenserede produkter, til markedsføring, til at forbedre it-sikkerhed, til kommunikation og til udvikling af de licenserede produkter.

I KAILA udføres behandlingen af personoplysninger i samtaler og uploadede dokumenter af Karnov Group som **databehandler** i overensstemmelse med kundens dokumenterede instruks i **databehandleraftalen** (artikel 28 i GDPR). Kunden, som dataansvarlig, fastlægger retsgrundlaget for behandlingen af personoplysninger i KAILA.

### 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 registreredes rettigheder i vores **privatlivspolitik**.

### 8.5 Tredjeparters behandling af personoplysninger

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 selvstændig dataansvarlig,** kan tredjeparter behandle begrænsede personoplysninger, der er nødvendige for at levere platformen og sikre dens sikre drift.

**Når Karnov Group fungerer som databehandler på vegne af en kunde,** vil visse godkendte **underdatabehandlere** gemme og behandle dataene for at levere tjenesten. Disse underdatabehandlere er:

**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 anvendes, forudsat at enhver udskiftning er inden for disse udbyderes nuværende serviceudbud og hostes under de samme EU/EØS-dataplaceringskontroller.

Brugen af disse underdatabehandlere, deres roller, hostingplaceringer og gældende sikkerhedsforanstaltninger er dokumenteret i **databehandleraftalen (DBA)** mellem Karnov Group og kunden. Denne aftale definerer det nøjagtige omfang af behandlingen, databeskyttelseskontroller og slettefrister, der gælder for data, der håndteres af underbehandlere.

Tilsyn med højrisiko-leverandører gennemgås årligt, leverandørers sikkerhedshændelser overvåges løbende, og indvirkningen af enhver hændelse på Karnov Groups information og tjenester vurderes straks.

# 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.

For samtaler, der ikke er fastgjort af brugeren, vil hver samtale være **tilgængelig for brugeren i 90 dage efter den seneste aktivitet og derefter blive slettet**, medmindre brugeren sletter den tidligere. Fastgjorte samtaler opbevares, indtil de enten slettes aktivt af brugeren eller indtil kundeaftalen ophører. Dette giver brugeren mulighed for at genbesøge tidligere input eller stille yderligere spørgsmål om det samme emne. **Når en samtale slettes, slettes alle dokumenter, der er uploadet inden for den pågældende samtale, også.**

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-funktioner.

- **Betjenelige:** Alle interaktioner og navigation kan udføres via tastatur og skærmlæsere.
- **Forståelige:** Kommunikation og funktioner er klare og intuitive, så alle brugere 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 de licenserede produkter er ikke specifikt optimeret til mobil brug. For en komplet oversigt over understøttede browsere, besøg vores **side om browserkompatibilitet.**

Der kræves internetforbindelse for at 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 handlemulighed og menneskeligt tilsyn

KAILA er designet som et hjælpemiddel, der understøtter, **men ikke** erstatter, menneskelig beslutningstagning. Det er underlagt menneskelig kontrol og tilsyn og træffer ikke automatiserede beslutninger, der har væsentlig indflydelse på enkeltpersoners grundlæggende rettigheder, sundhed eller sikkerhed. Brugerne informeres via brugergrænsefladen og brugerbetingelserne om, at det kun skal bruges som et hjælpeværktøj 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 Teknologisk 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 svarene.

Samlet 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 Privatlivets fred og datastyring

KAILA opretholder privatliv og stærk datastyring gennem dataminimering, security-by-design og tydelig styring af en applikations livscyklus. 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@karnovgroup.com.

### 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-forskelsbehandling og retfærdighed

KAILAs rolle som et værktøj til beslutnings under menneskelig overvågning 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 ligeværdig anvendelse i forskellige sagsbehandlingssammenhænge, samtidig med at mennesker bevarer kontrollen over de endelige beslutninger.

## 12.6 Social 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 opretholder 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, kun intern adgang til systemer, 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 persondatasikkerheden og præciserer i sine licensvilkår, 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 underrette kunden i tilfælde af et brud på databeskyttelsen, der vedrører kundens bruger, uden unødig forsinkelse.

## 13.2 Ansvar og erstatning

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

# 14. Revisionslog

| **Version** | **Gyldig fra** | **Revisionskategori Ny/Opdatering/Formulering/Ingen** | **Beskrivelse af vigtigste revisioner** |
|---|---|---|---|
| 1.0 | 01.09.2024 | Ny | Udarbejdelse af KAILA Compliance Whitepaper baseret på brugeres spørgsmål. |
| 2.0 | 10.01.2025 | Opdatering | Ny struktur af hvidbogen, så den passer til ISO27000-rammen, og tilføjelse af detaljer til de specifikke emner. |
| 3.0 | 05.09.2025 | Opdatering | Opdatering for at matche ny upload-funktion og dokumentanalysefunktion, herunder ændring af roller vedrørende behandling af personoplysninger |
| | | | |