Risika for AI – Privacy Policy

Version 2.0 · Effective 6 November 2026 · Risika A/S

1. About this policy

This policy explains how Risika A/S processes personal data in Risika for AI: access to Risika's company and credit data through AI assistants via Risika's MCP server, including Microsoft 365 Copilot, Claude and ChatGPT.

It supplements Risika's general privacy policy (risika.com/privacy), which applies to Risika's other services, our website and our customer relationships.

2. Who we are

The data controller is Risika A/S, CVR 37677892, Danneskiold-Samsøes Allé 41, 1434 Copenhagen K, Denmark. Contact: contact@risika.com. Our external Data Protection Officer can be reached at dpo@risika.com.

3. How Risika for AI works

- A user asks a question in the AI assistant.
- The AI assistant sends a request to Risika's MCP server. The request contains the name of the function used and the search parameters needed to answer, such as a company name or company registration number.
- The MCP server retrieves the answer from Risika's platform using the user's own Risika login and subscription rights, and returns it to the AI assistant.

Risika's servers are located in the EU, and traffic to them passes through Cloudflare (see sections 7 and 8). Risika does not receive the user's conversation, files, emails or other content from the AI assistant, only the request parameters needed to answer.

4. Microsoft 365 Copilot

Risika for AI is available in Microsoft 365 Copilot. When a user uses Risika for AI in Copilot:

- Risika's answer is processed in the customer's own Microsoft 365 environment. Microsoft processes it on behalf of the customer under the customer's agreement with Microsoft, not on behalf of Risika.
- Risika has no access to the customer's Microsoft 365 environment, including emails, documents, chats or calendars.
- Risika does not index or store Risika data in Microsoft 365. Data is fetched live when the user asks.
- Content that Copilot creates with Risika data, for example a Word document or an email, is controlled by the customer.

Microsoft's processing is governed by Microsoft's own terms and privacy statement (privacy.microsoft.com). The same principle applies to other AI assistants, such as Claude (Anthropic) and ChatGPT (OpenAI): the provider processes data under its agreement with the customer.

5. Personal data about users of Risika for AI

What we process: name and business email of the user, the customer the user belongs to, a user id, IP address, time of the request, the function used, what was looked up (a company or a person) and the status of the request. For pilot customers, we also process the user's job title and the record of the user's acceptance of the terms.

Purposes and legal bases:

- To provide Risika for AI under the customer's agreement with Risika, including the pilot sign-up and acceptance of the terms: our legitimate interest in delivering the service (GDPR art. 6(1)(f)).
- To keep a record of who has received credit information, as required by the conditions of Datatilsynet's authorisation for credit information activities and corresponding Swedish rules: legal obligation (GDPR art. 6(1)(c)).
- To protect the service against security incidents and misuse, such as shared logins or bulk extraction: our legitimate interest (GDPR art. 6(1)(f)).

Retention: technical logs, including IP addresses, are kept for 12 months. The record of what was looked up, by whom and when is kept for 3 years. Records of lookups on beneficial owners are kept for 5 years. Account data is deleted 3 months after the user profile is closed, or after 3 years of inactivity, as described in our general privacy policy.

6. Persons in our company data: purposes and legal basis

Company information in Risika for AI may include natural persons, such as directors, board members, founders, legal owners and sole traders.

Sources: public business registers (Erhvervsstyrelsen in Denmark, Bolagsverket in Sweden, Brønnøysundregistrene in Norway and PRH in Finland) and published annual accounts.

6.1 Credit and risk assessment and customer due diligence. Information about persons in our company data, such as their roles in and ownership of companies, is processed to assess the financial solvency and creditworthiness of companies and to support our customers' customer due diligence. The legal basis is Article 6(1)(f) of the GDPR and section 20 of the Danish Data Protection Act, under our authorisations as a credit information agency from Datatilsynet (Denmark) and Integritetsskyddsmyndigheten (Sweden).

6.2 Company events for sales and market purposes (new in version 2.0). We also use information about persons' roles and legal ownership in companies from public business registers to identify company-level events, such as a change of chief executive or owner. Your AI assistant can retrieve these events for business-to-business sales and market purposes. The events contain no names, identity numbers, addresses or contact details of persons. They exclude sole traders and are not derived from beneficial-owner information. Danish companies registered with advertisement protection (reklamebeskyttelse) in CVR are included but marked as advertisement-protected, and their CVR phone number and email address are not provided for marketing. The legal basis is our and our customers' legitimate interest under Article 6(1)(f) of the GDPR. This processing is separate from our credit information activity and is not carried out under section 20 of the Danish Data Protection Act or our credit information authorisations. Company events are kept for up to 18 months.

6.3 Your use of the output. When your AI assistant retrieves information from Risika, you are an independent controller for your further use of it. Company events may not be used for credit

assessment. Outreach based on them must comply with applicable marketing law, including the advertisement protection marked on a company and the recipient's right to opt out.

6.4 Right to object. A person may object at any time to the processing described in 6.2. We will then stop using information about that person to generate company events. Contact dpo@risika.com.

6.5 Safeguards in Risika for AI. Whatever the purpose:

- Beneficial owners are shown only as a number, never by name.
- Persons with protected identity are shown without name or address.
- Swedish personal identity numbers are not included in answers.
- Home addresses are not included in standard answers.
- Lookups on persons require the user to be signed in personally and are limited in number.

7. Recipients

Answers are delivered only to authorised users of Risika's customers. Risika uses the following data processors for Risika for AI:

- Amazon Web Services (AWS): hosting, databases and logs on Risika's servers in the EU.
- Cloudflare: protects and routes traffic to Risika's MCP server (mcp.risika.com).
- Google Workspace: email, including messages to contact@risika.com and dpo@risika.com.
- HubSpot: pilot sign-up and acceptance of the terms, and the user's name, work email, job title and company as part of the customer relationship.
- Mailjet: sign-in and password-reset emails.
- Auth0: sign-in and single sign-on (SSO).

All processors process data under data processing agreements with Risika. We disclose data to authorities where the law requires it. We do not sell personal data.

Risika does not use requests or answers in Risika for AI to train AI models. Our terms require customers to use AI assistants whose provider does not use Risika data to train models.

8. Transfers outside the EU/EEA

Risika's servers for Risika for AI are located in the EU. Cloudflare routes traffic through its global network, so data may pass through or be processed in countries outside the EU/EEA. HubSpot, Auth0 and Mailjet store Risika's data in the EU. Google, which provides Google Workspace, belongs to a group based in the United States and may process data outside the EU/EEA. Such transfers are covered by the EU-U.S. Data Privacy Framework and the EU Standard Contractual Clauses in our agreements with Cloudflare and Google. If a customer's AI provider processes data outside the EU/EEA, this happens under the customer's agreement with that provider.

9. Security and personal data breaches

If a personal data breach occurs in Risika for AI, Risika notifies the Danish Data Protection Agency (Datatilsynet) within 72 hours where required by GDPR art. 33, informs affected individuals without undue delay where the breach is likely to result in a high risk to them (art. 34), and informs affected customers without undue delay where the breach concerns their users' data.

10. Your rights

You have the right to access your personal data, including information about who has received it, and the right to rectification, erasure, restriction and objection, within the limits set by law. Contact us at contact@risika.com.

11. Complaints

You can complain to Datatilsynet, Carl Jacobsens Vej 35, 2500 Valby, Denmark (dt@datatilsynet.dk). If you are in Sweden, you can also complain to Integritetsskyddsmyndigheten (IMY), imy.se.

12. Changes and versions

The current version of this policy is always available at this address. Earlier versions are archived with their own address and as PDF. We will inform customers of material changes.

Version 2.0 adds company events for sales and market purposes (section 6.2), a section on personal data breaches (section 9) and further data processors (section 7).

Archived versions: version 2026.10.26 (effective 29 October 2026) (archived page, PDF) · version 1.0 (effective 16 October 2026) (archived page, PDF).

Risika for AI – Privatlivspolitik

Version 2.0 · Gældende fra 6. november 2026 · Risika A/S

1. Om denne politik

Denne politik beskriver, hvordan Risika A/S behandler personoplysninger i Risika for AI: adgang til Risikas virksomheds- og kreditdata gennem AI-assistenter via Risikas MCP-server, herunder Microsoft 365 Copilot, Claude og ChatGPT.

Den supplerer Risikas generelle privatlivspolitik (risika.com/privacy), som gælder for Risikas øvrige services, vores hjemmeside og vores kundeforhold.

2. Hvem vi er

Dataansvarlig er Risika A/S, CVR 37677892, Danneskiold-Samsøes Allé 41, 1434 København K. Kontakt: contact@risika.com. Vores eksterne databeskyttelsesrådgiver kan kontaktes på dpo@risika.com.

3. Sådan fungerer Risika for AI

- En bruger stiller et spørgsmål i AI-assistenten.
- AI-assistenten sender en forespørgsel til Risikas MCP-server. Forespørgslen indeholder navnet på den anvendte funktion og de søgeparametre, der skal til for at svare, fx et virksomhedsnavn eller et CVR-nummer.
- MCP-serveren henter svaret fra Risikas platform med brugerens eget Risika-login og abonnementsrettigheder og sender det tilbage til AI-assistenten.

Risikas servere står i EU, og trafikken til dem passerer gennem Cloudflare (se punkt 7 og 8). Risika modtager ikke brugerens samtale, filer, e-mails eller andet indhold fra AI-assistenten, kun de søgeparametre, der skal til for at svare.

4. Microsoft 365 Copilot

Risika for AI er tilgængelig i Microsoft 365 Copilot. Når en bruger anvender Risika for AI i Copilot:

- Behandles Risikas svar i kundens eget Microsoft 365-miljø. Microsoft behandler det på kundens vegne efter kundens aftale med Microsoft, ikke på Risikas vegne.
- Har Risika ikke adgang til kundens Microsoft 365-miljø, herunder e-mails, dokumenter, chats eller kalendere.
- Indekserer eller gemmer Risika ikke Risika-data i Microsoft 365. Data hentes direkte, når brugeren spørger.
- Er indhold, som Copilot frembringer med Risika-data, fx et Word-dokument eller en e-mail, under kundens kontrol.

Microsofts behandling er omfattet af Microsofts egne vilkår og privatlivserklæring (privacy.microsoft.com). Det samme princip gælder for andre AI-assistenter, fx Claude (Anthropic) og ChatGPT (OpenAI): leverandøren behandler data efter sin aftale med kunden.

5. Personoplysninger om brugere af Risika for AI

Hvad vi behandler: brugerens navn og arbejdsmail, den kunde, brugeren hører til, et bruger-ID, IP-adresse, tidspunktet for forespørgslen, den anvendte funktion, hvad der er slået op (en virksomhed eller en person) og forespørgslens status. For pilotkunder behandler vi også brugerens stillingsbetegnelse og registreringen af brugerens accept af vilkårene.

Formål og retsgrundlag:

- At levere Risika for AI efter kundens aftale med Risika, herunder tilmelding til pilotforløb og accept af vilkårene: vores legitime interesse i at levere servicen (GDPR art. 6, stk. 1, litra f).
- At registrere, hvem der har modtaget kreditoplysninger, som krævet efter vilkårene i Datatilsynets tilladelse til kreditoplysningsvirksomhed og tilsvarende svenske regler: retlig forpligtelse (GDPR art. 6, stk. 1, litra c).
- At beskytte servicen mod sikkerhedshændelser og misbrug, fx delte logins eller masseudtræk: vores legitime interesse (GDPR art. 6, stk. 1, litra f).

Opbevaring: Tekniske logs, herunder IP-adresser, opbevares i 12 måneder. Registreringen af, hvad der er slået op, af hvem og hvornår, opbevares i 3 år. Registreringer af opslag på reelle ejere opbevares i 5 år. Kontooplysninger slettes 3 måneder efter, at brugerprofilen er lukket, eller efter 3 års inaktivitet, som beskrevet i vores generelle privatlivspolitik.

6. Personer i vores virksomhedsdata: formål og retsgrundlag

Virksomhedsoplysninger i Risika for AI kan omfatte fysiske personer, fx direktører, bestyrelsesmedlemmer, stiftere, legale ejere og indehavere af enkeltmandsvirksomheder.

Kilder: offentlige erhvervsregistre (Erhvervsstyrelsen i Danmark, Bolagsverket i Sverige, Brønnøysundregistrene i Norge og PRH i Finland) og offentliggjorte årsregnskaber.

6.1 Kredit- og risikovurdering og kundekendskab. Oplysninger om personer i vores virksomhedsdata, fx deres roller i og ejerskab af virksomheder, behandles for at vurdere virksomheders økonomiske soliditet og kreditværdighed og for at understøtte vores kunders kundekendskabsprocedurer. Retsgrundlaget er databeskyttelsesforordningens art. 6, stk. 1, litra f, og databeskyttelseslovens § 20 under vores tilladelser som kreditoplysningsbureau fra Datatilsynet (Danmark) og Integritetsskyddsmyndigheten (Sverige).

6.2 Virksomhedshændelser til salgs- og markedsformål (nyt i version 2.0). Vi bruger også oplysninger om personers roller i og legale ejerskab af virksomheder fra offentlige erhvervsregistre til at identificere hændelser på virksomhedsniveau, fx skift af administrerende direktør eller ejer. Din AI-assistent kan hente disse hændelser til salgs- og markedsformål mellem virksomheder. Hændelserne indeholder ingen navne, identifikationsnumre, adresser eller kontaktoplysninger på personer. Enkeltmandsvirksomheder er udeladt, og hændelserne bygger ikke på oplysninger om reelle ejere. Danske virksomheder, der er registreret med reklamebeskyttelse i CVR, indgår, men er markeret som reklamebeskyttede, og deres telefonnummer og e-mailadresse fra CVR udleveres ikke til markedsføring. Retsgrundlaget er vores og vores kunders legitime interesse, jf. databeskyttelsesforordningens art. 6, stk. 1, litra f. Behandlingen er adskilt fra vores kreditoplysningsvirksomhed og sker ikke efter databeskyttelseslovens § 20 eller vores tilladelser som kreditoplysningsbureau. Virksomhedshændelser opbevares i op til 18 måneder.

6.3 Din brug af svarene. Når din AI-assistent henter oplysninger fra Risika, er du selvstændigt dataansvarlig for din videre brug af dem. Virksomhedshændelser må ikke bruges til kreditvurdering. Henvendelser på baggrund af dem skal overholde gældende markedsføringsregler, herunder den

reklamebeskyttelse, en virksomhed er markeret med, og modtagerens ret til at frabede sig henvendelser.

6.4 Ret til indsigelse. En person kan til enhver tid gøre indsigelse mod behandlingen i punkt 6.2. Vi holder så op med at bruge oplysninger om personen til at danne virksomhedshændelser. Kontakt dpo@risika.com.

6.5 Beskyttelse i Risika for AI. Uanset formål gælder:

- Reelle ejere vises kun som et antal, aldrig med navn.
- Personer med beskyttet identitet vises uden navn og adresse.
- Svenske personnumre indgår ikke i svarene.
- Hjemmeadresser indgår ikke i standardsvar.
- Opslag på personer kræver, at brugeren er logget ind personligt, og antallet er begrænset.

7. Modtagere

Svar leveres kun til autoriserede brugere hos Risikas kunder. Risika anvender følgende databehandlere til Risika for AI:

- Amazon Web Services (AWS): hosting, databaser og logs på Risikas servere i EU.
- Cloudflare: beskytter og dirigerer trafikken til Risikas MCP-server (mcp.risika.com).
- Google Workspace: e-mail, herunder henvendelser til contact@risika.com og dpo@risika.com.
- HubSpot: tilmelding til pilotforløb og accept af vilkårene samt brugerens navn, arbejdsmail, stillingsbetegnelse og virksomhed som led i kundeforholdet.
- Mailjet: e-mails ved login og nulstilling af adgangskode.
- Auth0: login og single sign-on (SSO).

Alle databehandlere behandler data efter databehandleraftaler med Risika. Vi videregiver oplysninger til myndigheder, når loven kræver det. Vi sælger ikke personoplysninger.

Risika bruger ikke forespørgsler eller svar i Risika for AI til at træne AI-modeller. Vores vilkår kræver, at kunderne bruger AI-assistenter, hvis leverandør ikke bruger Risika-data til at træne modeller.

8. Overførsel uden for EU/EØS

Risikas servere til Risika for AI står i EU. Cloudflare dirigerer trafikken gennem sit globale netværk, så data kan passere gennem eller blive behandlet i lande uden for EU/EØS. HubSpot, Auth0 og Mailjet opbevarer Risikas data i EU. Google, der leverer Google Workspace, tilhører en koncern med hjemsted i USA og kan behandle data uden for EU/EØS. Sådanne overførsler er omfattet af EU-U.S. Data Privacy Framework og EU's standardkontraktbestemmelser i vores aftaler med Cloudflare og Google. Hvis en kundes AI-leverandør behandler data uden for EU/EØS, sker det efter kundens aftale med leverandøren.

9. Sikkerhed og brud på persondatasikkerheden

Hvis der sker et brud på persondatasikkerheden i Risika for AI, anmelder Risika det til Datatilsynet inden for 72 timer, når det kræves efter databeskyttelsesforordningens art. 33. Risika underretter de berørte personer uden unødig forsinkelse, når bruddet sandsynligvis indebærer en høj risiko for dem

(art. 34), og underretter berørte kunder uden unødig forsinkelse, når bruddet vedrører deres brugeres data.

10. Dine rettigheder

Du har ret til indsigt i dine personoplysninger, herunder oplysning om, hvem der har modtaget dem, og ret til berigtigelse, sletning, begrænsning og indsigelse inden for lovens rammer. Kontakt os på contact@risika.com.

11. Klage

Du kan klage til Datatilsynet, Carl Jacobsens Vej 35, 2500 Valby (dt@datatilsynet.dk). Hvis du er i Sverige, kan du også klage til Integritetsskyddsmyndigheten (IMY), imy.se.

12. Ændringer og versioner

Den gældende version af politikken findes altid på denne adresse. Tidligere versioner arkiveres med egen adresse og som PDF. Vi orienterer kunderne om væsentlige ændringer.

Version 2.0 tilføjer virksomhedshændelser til salgs- og markedsformål (punkt 6.2), et afsnit om brud på persondatasikkerheden (punkt 9) og yderligere databehandlere (punkt 7).

Arkiverede versioner: version 2026.10.26 (gældende fra 29. oktober 2026) (arkiveret side, PDF) · version 1.0 (gældende fra 16. oktober 2026) (arkiveret side, PDF).