

AI og revisjon: Fremtiden er her. Tenk deg et system som aldri tar pause, og som alltid er på vakt mot feil og avvik – helt uten menneskelig innblanding. I denne faste spalten tar vi pulsen på hvordan kunstig intelligens endrer revisjonsbransjen. Er du klar for å bli kjent med morgendagens digitale kollegaer?

Revisjonsfirmaets skjulte AI-risiko

FOR REVISJONSFIRMAER ER DEN STØRSTE AI ACT-RISIKOEN DIGITALT FREMOVERLENTE PERSONALLEDERE

Dagens generelle AI-assistenten er ikke ment for bruk i AI Act høyrisiko-aktiviteter. Samtidig er de teknisk fullt kapable til å rangere jobbsøkere, fordele oppdrag til ansatte, eller anbefale bonus. Et revisjonsfirma som bruker ikke-høyrisiko-AI-systemer på personalleder-oppgaver, kan selv bli pålagt de tunge samsvarspliktene som gjelder for leverandører av høyrisiko-AI. Kjerneoppgavene i revisjon er ikke omfattet av AI Acts høyrisikoliste, men forordningen gir nyttige oppskrifter for intern AI-styring.



Ph.D.
Lars Erlend Leganger
Chief Technical Officer
Advokatfirmaet PwC



Magnus Haukeberg Skaar
Director
PwC

AI-assistenten får en ny jobb

Du jobber i et digitalt fremoverlent revisjonsfirma, der alle ansatte har fått tilgang på en språkmodellbasert generell AI-assistent, og grundig opplæring i hvordan den skal – og ikke skal – brukes i revisjon. Samtidig sitter en personalleder med altfor mange jobbsøknader og altfor lite tid til å velge ut dem som skal slippe videre i prosessen. AI til unnsetning!

Først får AI-assistenten beskjed om å hente ut utdanning, arbeidserfaring, autorisasjoner og språkferdigheter til faste kolonner. Originalsøknaden følger med, og hvert datafelt kan kontrolleres mot kilden. Så kommer et tilsynelatende naturlig oppfølgingsprompt: «Gi kandidaten poeng for egnethet opp mot stillingsbeskrivelsen, vurder kulturell match, og lag en detaljert presentasjon av de ti beste.»

Språkmodellen og brukergrensesnittet er det samme, men oppgavene er forskjellige. Den første oppgaven er å strukturere informasjon. Den andre innebærer evaluering av mennesker og kan påvirke hvem som kalles inn til intervju.

Det skillet er kjernen i EUs AI Act – KI-forordningen på norsk – som skal gjennomføres i norsk rett gjennom en egen KI-lov. Regelverket klassifiserer ikke risiko ut fra hvor avansert AI-teknologien er, det ser først og fremst på hva AI-systemet er tilsiktet brukt til, i hvilken sammenheng og med hvilken virkning.

For et ordinært revisjonsfirma ligger den mest nærliggende eksponeringen for høyrisikoreglene i AI Act ikke i kjernevirksomheten, men i personalledelse.

Mer tid, samme retning

AI Act trådte i kraft i EU 1. august 2024, men bestemmelsene fases gradvis inn. Etter endringsforordningen fra juli 2026 skal reglene om høyrisiko-AI-systemer etter artikkel 6 nr. 2 og vedlegg III anvendes fra 2. desember 2027.¹

I Norge er KI-forordningen ennå ikke gjennomført. Regjeringen opplyste 4. august 2026 at et oppdatert forslag til KI-lov skal sendes på ny høring høsten 2026, og at ambisjonen er å fremme loven for Stortinget våren 2027. Arbeidet med innlemmelse i EØS-avtalen og nødvendige EØS-tilpasninger pågår.² For norske foretak med virksomhet, bruk eller leveranser inn mot EU må forordningens geografiske virkeområde vurderes særskilt – norsk gjennomføring er ikke nødvendigvis den eneste relevante tidslinjen.

Utsettelsen gir mer tid, men gjør ikke klassifiseringsspørsmålet mindre aktuelt. Systemer som utvikles eller kjøpes nå, vil typisk være i bruk når reglene får anvendelse, og tilsiktet formål, arbeidsflyt, datagrunnlag og rollefordeling kan være vanskelig å rekonstruere lenge etter at løsningen er blitt en del av hverdagen.

¹ Europaparlaments- og rådsforordning (EU) 2024/1689 av 13. juni 2024 om harmoniserte regler for kunstig intelligens (AI Act), EUT L, 2024/1689, 12.7.2024, og forordning (EU) 2026/1744, særlig endringen av artikkel 113. Reglene i kapittel III avsnitt 1-3 skal anvendes fra 2. desember 2027. eur-lex.europa.eu.

² Digitaliserings- og forvaltningsdepartementet, «Tung vil sende KI-loven med endringer på høring», pressemelding 4. august 2026, regjeringen.no. Om forordningens geografiske virkeområde: AI Act artikkel 2.

Personalledelse er høyrisiko i AI Act

AI Acts vedlegg III er en liste over brukstilfeller forordningen identifiserer som høyrisiko. Revisjons-, regnskaps- eller rådgivningstjenester står ikke på listen: For revisjonsfirmaer er punkt 4 om ansettelse og arbeidstakerstyring det klart mest nærliggende området.³ Listen omfatter blant annet AI-systemer som brukes til:

- 1. målretting av konkrete stillingsannonser;
- 2. analyse, filtrering og evaluering av søkere;
- 3. beslutninger om arbeidsvilkår, forfremmelse og avslutning av arbeidsforhold;
- 4. oppgavefordeling basert på individuell atferd eller personlige kjennetegn; og
- 5. overvåking eller evaluering av ansattes prestasjon og atferd.

Oversatt til revisjonsfirmaets hverdag betyr dette kandidatsøk, CV-rangering, intervju- og testscoring, bemanning av oppdrag, måling av faktureringsgrad og kvalitet, bonus, opprykk, partnerløp, forbedringsplaner og avslutning av arbeidsforhold.⁴

Kommisjonens ikke-bindende utkast til klassifiseringsveiledning har et relevant eksempel: Et advokatfirma som bruker fakturerte timer, tidligere leveringstid, respons på e-post og frivillig deltakelse i opplæring og klientutvikling for å score advokatfullmektinger og fordele klientoppdrag. Utkastet plasserer systemet i vedlegg III punkt 4(b). Eksempelet er illustrerende, ikke normerende, men det er vanskelig å se en prinsipiell forskjell mellom dette og om et revisjonsfirma bruker faktureringsgrad, leveringstid, kvalitetsfunn, klienttilbakemeldinger og intern feedback til å gjøre performance-

Personalleder-oppgave	Hva AI-systemet gjør	AI Act risikoklassifisering
CV-uttrekk	Henter navn, datoer, utdanning og sertifikater til faste felt	Kan falle utenfor etter unntaket i artikkel 6 nr. 3 dersom funksjonen bare er prosedyremessig eller forberedende og ikke profilerer – men unntaket må vurderes og dokumenteres av den som er leverandør
Kandidatscoring	Gir poeng for erfaring, utdanning, språk eller forventet egnethet	Normalt høyrisiko; evalueringen kan være profilering selv når kriteriene er transparente
Bemanning etter kapasitet	Matcher tilgjengelighet, geografi og nødvendige autorisasjoner	Normalt utenfor punkt 4(b) når kriteriene er nøytrale og systemet ikke evaluerer personen
Bemanning etter prestasjon	Rangerer medarbeidere etter fakturering, kvalitet, responstid eller klientvurderinger	Høyrisiko etter punkt 4(b)
Kompensasjon og opprykk	Gir score, prognose eller anbefaling som påvirker beslutning om kompensasjon og opprykk	Høyrisiko etter punkt 4(b); profilering

vurderinger, bestemme bonus, eller planlegge bemanning på revisjonsoppdrag med hjelp av AI-assistenter.⁵

Grensedragningen går ved AI-systemets funksjon: Ren kapasitetsplanlegging etter selvrapportert tilgjengelighet, geografi, nødvendig autorisasjon og objektive uavhengighetsbegrensninger kan falle utenfor høyrisiko-kategorisering. Men om systemet vurderer hvem som er mest pålitelig, produktiv eller lovende, har det en høyrisiko-rolle.

De tyngste pliktene ligger hos leverandøren

AI Act skiller mellom leverandøren av et AI-system og idriftsetteren av det – virksomheten som bruker systemet under egen myndighet. Leverandøren bærer de tyngste system- og samsvarsforplik-

telsene. For et høyrisikosystem omfatter disse blant annet risikostyring, data- og datastyring, teknisk dokumentasjon, logging, informasjon til brukeren, design for menneskelig kontroll, nøyaktighet, robusthet, cybersikkerhet, kvalitetsstyring, samsvarsvurdering, registrering og oppfølging etter at systemet er tatt i bruk.⁶

Idriftsetteren slipper ikke helt unna. Et revisjonsfirma som kjøper et ferdig høyrisikosystem, må blant annet bruke det etter instruksjonene, legge menneskelig kontroll til personer med nødvendig kompetanse, opplæring, myndighet og støtte, overvåke bruken, håndtere relevante inputdata, oppbevare logger

3 Forordning (EU) 2024/1689, vedlegg III punkt 4 bokstav a og b.
4 Noen HR-nære bruksmåter er ikke bare regulert, men forbudt: AI Act artikkel 5 rammer AI-systemer som utleder følelser hos ansatte og arbeidssøkere, og forbudet har gjeldt siden februar 2025. Og AI Act er ikke det eneste regelverket – kandidatscoring og prestasjonsmåling møter allerede i dag personvernforordningens regler om profilering og automatiserte avgjørelser, arbeidsmiljøloven kapittel 9 om kontrolltiltak og drøfting med tillitsvalgte, og diskrimineringsvernet når kriterier som «kulturell match» slår ulikt ut.

5 Europakommisjonen, *Draft guidelines for the classification of high-risk AI systems*, publisert 19. mai 2026, digital-strategy.ec.europa.eu. Retningslinjene var fortsatt utkast og er ikke bindende.

6 Forordning (EU) 2024/1689, særlig artikkel 9–15 (krav til høyrisikosystemer), artikkel 16 og 17 (leverandørens plikter og kvalitetsstyringssystem), artikkel 43 (samsvarsvurdering), artikkel 47–49 (samsvarserklæring, CE-merking og registrering) og artikkel 72 (overvåking etter at systemet er tatt i bruk).

og informere ansatte før systemet brukes på arbeidsplassen.⁷

I tillegg kommer rettighetene til dem systemet brukes på. Den som berøres av en beslutning som treffes på grunnlag av output fra et høyrisikosystem i vedlegg III, og som har rettsvirkning eller tilsvarende betydelig virkning, kan etter artikkel 86 kreve en forklaring på systemets rolle i beslutningen. For HR betyr det at både kandidater og ansatte kan be om å få vite hvilken vekt systemet faktisk hadde.

Likevel er rolleforskjellen vesentlig. Idriftsetteren skal normalt operere et system som leverandøren allerede har klassifisert, dokumentert og utviklet for den aktuelle bruken. Det er leverandøren som står ansvarlig for at systemet oppfyller kravene.

Men generelle AI-verktøy kan brukes til så mangt. Hva skjer når et ikke-høyrisikosystem tas i bruk på et høyrisikoområde? Da må vi til AI Act artikkel 25.

Ved feil bruk får idriftsetteren leverandøransvaret

Artikkel 25 nr. 1 bokstav c sier at en distributør, importør, idriftsetter eller annen tredjepart skal anses som leverandør dersom den endrer det tilsiktede formålet til et tidligere ikke-høyrisikosystem – uttrykkelig også et AI-system med generelt formål – slik at systemet blir et høyrisikosystem etter artikkel 6.⁸

Denne bestemmelsen er spesielt aktuell for generelle AI-assistenter. Den opprinnelige leverandøren kan tilby dem for generell tekstproduksjon, oppsummering og kunnskapsarbeid, uten et dokumentert formål om å evaluere kandidater og ansatte eller støtte andre høyrisikoaktiviteter. Hvis et revisjonsfirma bygger en slik assistent inn i en fast

arbeidsflyt for kandidatscoring, prestasjonsmåling, bemanning, bonus eller opprykk, kan revisjonsfirmaet ha gitt systemet et nytt tilsiktet formål. Da kan firmaet selv få leverandørforpliktelsene for et høyrisikosystem.

En enkelt eksperimentell prompt er ikke nødvendigvis nok. Vurderingen må knyttes til hvordan løsningen faktisk er konfigurert, dokumentert, integrert og satt i drift. Men en organisert løsning med faste instruksjoner eller prompter, definerte datakilder, automatisert rangering, HR-integrasjon og en etablert beslutningsrolle begynner raskt å ligne et system med et nytt formål – ikke tilfeldig feilbruk av en generell AI-assistent.

Dersom den opprinnelige leverandøren uttrykkelig har utelukket at systemet skal brukes til høyrisikoppgaver, har leverandøren etter artikkel 25 nr. 2 ikke plikt til å samarbeide eller utlevere dokumentasjon. Revisjonsfirmaet kan dermed pådra seg leverandøransvaret uten å få tilgang til det tekniske underlaget som trengs for å oppfylle det.

Brudd på kravene til høyrisikosystemer kan sanksjoneres med overtredelsesgebyr på inntil 15 millioner euro eller tre prosent av samlet global årsomsetning. Gebyrene rammer også når leverandørrollen har oppstått utilsiktet.

Risikoen kan håndteres. Tre grep er særlig aktuelle: kreve dokumentert høyrisikosamsvar fra leverandører av AI-systemer som er tiltenkt bruk i personalledelsesprosesser; avtalefeste tilgang til teknisk dokumentasjon og samarbeid dersom idriftsetteren likevel skulle pådra seg leverandøransvar; og – ikke minst – innføre policyer og opplæring som utvetydig forbyr bruk av generelle AI-verktøy til scoring, rangering og prestasjonsvurdering.

Seks kontrollspørsmål før du bruker AI i høyrisiko-områder

Risikoen tatt i betraktning kunne det være fristende kort og greit å forby all bruk av AI innen personalledelse. Det ville imidlertid være å skyte spurv med kanon – det er mange store og små oppgaver som helt uproblematisk kan løses av AI, og AI Act artikkel 6 nr. 3 gir en «sikkerhetsventil» som åpner for

enkelte slike anvendelser. En mulig operasjonalisering av unntaksmekanismen i artikkel 6 nr. 3 bokstav a og d – for henholdsvis «snever prosedyremessig oppgave» og «forberedende oppgave til en vurdering» – er å måle den tiltenkte bruken opp mot seks kontrollspørsmål:⁹

- 1. Profilerer systemet en fysisk person?** Profilerer er automatisert behandling av personopplysninger for å vurdere personlige aspekter ved et menneske, slik begrepet er definert i personvernforordningen artikkel 4 nr. 4. For systemer som evaluerer personlige aspekter som arbeidsprestasjon, kvalifikasjoner, pålitelighet eller atferd i vedlegg III-områder, er unntaksmuligheten i artikkel 6 nr. 3 stengt.
- 2. Er oppgaven konkret og avgrenset?** Input, behandling og output må kunne beskrives presist. «Støtte rekruttering» er for vidt. «Hente utdanning og sertifikater til faste felt» er avgrenset.
- 3. Endrer systemet form på informasjon, eller vurderer det betydningen av den?** Syntaktisk strukturering, dublett-kontroll og datauttrekk kan kvalifisere til unntak, men ikke relevansvurdering, scoring og risikoklassifisering.
- 4. Kan outputen påvirke utfallet?** Dersom systemet snevrer inn kandidatlisten, styrer oppmerksomheten eller forhåndsstrukturere vurderingen, er rollen neppe bare prosedyremessig eller rent saksforberedende. At et menneske fatter den formelle beslutningen til slutt, er ikke tilstrekkelig for å få unntak fra høyrisikoklassifisering.
- 5. Kan resultatet kontrolleres i praksis?** Teoretisk etterprøvbarehet er ikke nok. Brukeren må ha tilgang til kildene, nødvendig kompetanse, tid og et grensesnitt som gjør kontroll av AI-systemets handlinger mulig.
- 6. Inviterer outputen til kontroll og selvstendig vurdering?** Faktafelt uten handlingssignal kan være forholdsvis robuste. Poeng, rangeringer, sannsynligheter, fargekoder og «viktigste funn» skaper kognitive snarveier og øker faren for at systemets anbefaling følges ukritisk.

7 Forordning (EU) 2024/1689, artikkel 26 om idriftsetters plikter. Se også artikkel 14 om menneskelig kontroll og artikkel 86 om retten til forklaring av enkeltbeslutninger.

8 Forordning (EU) 2024/1689, artikkel 25 nr. 1 bokstav c og fortalepunkt 84. Bestemmelsen omfatter uttrykkelig endret tilsiktet formål for et AI-system med generelt formål. Se også samarbeidsregelen i artikkel 25 nr. 2, som endret ved forordning (EU) 2026/1744.

9 Lars Erlend Leganger, *When is an AI system high-risk? Operationalising the "no significant risk" carve-outs of the AI Act's Article 6(3)(a) and (d)*, masteroppgave, Universitetet i Oslo, 2026, særlig s. 9–13, 29–38 og 53–56. Tilgjengelig på [Nasjonalt vitenarkiv](#).

Bruk av artikkel 6 nr. 3-unntakene skal registreres i en EU-database. Dette gjelder også for idriftsettere med leverandøransvar gjennom mekanismen i artikkel 25.

Revisjon står utenfor høyrisiko-listen

Vedlegg III nevner ikke ordinær finansiell revisjon. AI-verktøy for planlegging, risiko for vesentlig feilinformasjon, bilagstesting, avviksanalyse, kontraktsanalyse, revisjonsutvalg, vurdering av revisjonsbevis, estimer, fortsatt drift og utkast til revisjonsberetning er ikke høyrisikosystemer etter denne klassifiseringsruten. Det er kun en AI Act juridisk avgrensning, ikke et generelt revisjonsprofesjonsfaglig AI-frislipp.

Det betyr ikke at AI Act aldri gjelder for revisjon. Artikkel 4 oppstiller en generell plikt til å støtte utviklingen av AI-kompetanse hos ansatte og andre som bruker AI-systemer på virksomhetens vegne, dette gjelder også utenfor høyrisikokategorien. Kommisjonens spørsmål og svar om AI-kompetanse understreker at tiltakene bør tilpasses virksomhetens rolle, systemets risiko, brukskonteksten og personenes eksisterende kunnskap. Det finnes ikke én obligatorisk kursform eller et generelt sertifikat. En intern oversikt over opplæring og andre veiledningstiltak kan brukes som dokumentasjon.¹⁰

I revisjon bør AI-opplæring knyttes til de konkrete oppgavene og de konkrete feilrisikoene i hver enkelt oppgave. Den som bruker et kontraktsverktøy, bør kjenne hvilke klausuler modellen typisk overser, hvordan hvert felt spores til kilden, hvilke avvik som utløser full manuell gjennomgang, og når systemet skal tas ut av bruk. AI-kompetanse er evnen til å forstå, kontrollere og dokumentere dine konkrete bruksområder – og kompetansen til å stoppe bruken om det trengs.

10 Europakommisjonen, *AI Literacy – Questions & Answers*, digital-strategy.ec.europa.eu. Se særlig spørsmålene om risikobasert opplæring, dokumentasjon og opplæring av personer som fører menneskelig kontroll.

AI Acts metodikk kan også brukes for intern AI-styring

Et system som trekker ut oppsigelsesklausuler fra kontrakter, og et system som gir kontraktene rød, gul eller grønn risiko for feil inntektsføring, ligger begge utenfor AI Act vedlegg III, men de har svært forskjellig påvirkning for revisjonen. Det første strukturerer informasjon. Det andre styrer hvilke undersøkelser revisor gjør først, og hva som lettere kan bli oversett. Revisjonsfirmaets interne AI-styring må se forskjellen i risiko, også der AI Act ikke gjør det.

En praktisk intern kontrollstige kan se slik ut:

Intern AI-risikokategori	Typisk AI-bruk i revisjon	Eksempler på kontroller
Prosedyremessige oppgaver og forberedelsesstøtte	Optisk tegngjenkjenning (OCR), transkripsjon, oversettelse, datauttrekk med kildepor	Godkjent verktøy, databehandlingsregler, kildereferanser, stikkprøver og grunnleggende logging
Vurderings- og beslutningsstøtte	Sammendrag, relevans-sortering, risikoscore, anbefalt utvalg og forslag til faglig behandling	Dokumentert brukstilfelle, validering mot representative saker, kontroll av både høye og lave risikoscorer, versjonsstyring, fullstendige logger og definerte stoppkriterier
Autonome handlinger i systemer	AI som sender forespørsler, endrer arbeidsfiler, åpner og lukker oppgaver	Tilganger begrenset til det systemet faktisk trenger, avgrensede fullmakter, godkjenning før vesentlige handlinger, reversible transaksjoner, løpende overvåking og hendelseshåndtering

Kontrollspørsmålene for AI Act artikkel 6 nr. 3 kan brukes analogisk til å plassere et revisjonsverktøy på denne stigen: Er oppgaven avgrenset? Bearbeider systemet data, eller vurderer det betydningen? Styrer det revisors oppmerksomhet? Kan outputen kontrolleres mot underliggende bevis? Tilrettelegger løsningen og forholdene rundt for selvstendig vurdering, eller ansporer den rask, ukritisk tilslutning?

Begynn med oppgaven, og dokumenter vurderingene om du bruker AI i personalledelse

Virksomheter bør ikke basere sin AI Act-etterlevelse på overordnet kartlegging av innkjøpte AI-løsninger. En og samme språkmodell er kapabel til å skrive e-post, hente data fra CV-er, rangere kandidater, analysere kontrakter og foreslå revisjonshandlinger, og produktnavnet forteller lite om regulatorisk og profesjonsfaglig risiko.

Start heller med oppgavene som utføres i virksomheten, og kartlegg hvilke AI-systemer som er tilgjengelige for hver enkelt oppgave. Dokumenter grundig vurderingene som ligger til grunn, om virksomheten åpner for bruk av generelle AI-assistenter i personalledelse gjennom unntaket i artikkel 6 nr. 3, for eksempel gjennom svar på de ovennevnte seks kontrollspørsmålene, og vær klar til å registrere slik bruk i EUs database når denne delen av AI Act trer i kraft.

For personalledelse kan kontrollspørsmålene avklare høyrisikokrav og avverge et uventet leverandøransvar. For revisjon kan kontrollspørsmålene brukes i intern AI-styring. Revisorer er vant til å dokumentere vurderinger de har gjort, ikke bare konklusjoner de har landet på. Den vanen er verdt å ta med seg inn i AI-styringen, både innenfor og utenfor AI Act. ●